



Function:	Group
Policy Reference:	GEN_GRO_04
Title:	Data Protection Policy
Purpose:	Outline the principles the Group must satisfy when obtaining, handling, Processing, transporting or storing Personal Data
Pages:	20

Version:	2
Issue date:	30/09/2024
Review due:	30/09/2026
Author:	Emma Versluys
Approver:	Joe Vorih





Scope

This policy applies to all employees and officers across the Group. The policy also applies to individuals on work experience, contractors, agents, consultants or any others working for or on behalf of Genuit Group plc (together "Company Personnel"). In this document, 'Genuit', 'Company' and 'Group' refers to Genuit Group plc and its subsidiaries. 'Our' and 'we' refers to Genuit Group.

This policy sets out what we expect from you in order for the Company to comply with its obligations under the relevant data protection laws. Your compliance with this policy is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this policy. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this policy may result in disciplinary action.

You must read, understand and comply with this policy when Processing Personal Data on our behalf. Where training is required in relation to Data Protection, you must complete such training. Training completion will be monitored and reported on at Group level.

This policy (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, customers or regulators without prior authorisation from the Company Secretary.

This policy does not form part of any employee's contract of employment and we may amend it at any time.

Definitions

Automated Decision-Making (ADM)	when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.
Automated Processing	any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.
Consent	agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.
Data Controllers	are the people who, or organisations which, determine the purposes for which, and the manner in which, Personal Data is Processed. They have a responsibility to establish practices and policies in line with the Data Protection Laws.
Data Subject	a living, identified or identifiable individual based within the European Union about whom we hold Personal Data and who may have legal rights regarding their Personal Data.
Data Processors	includes any person who Processes Personal Data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle Personal Data behalf of the Group.
GDPR/Data Protection Laws	a) To the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of personal data, including but not limited to the UK General Data Protection Regulation and the Data Protection Act 2018. b) To the extent the EU GDPR applies, the law of the European Union or any member state of the European Union, including but not limited to the General Data Protection Regulation ((EU) 2016/679) to which the Business Unit is subject, which relates to the protection of Personal Data.
ICO	The Information Commissioner's Office.
Personal Data	any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Category Personal Data and

	Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
Process/Processing/Processed/Processes	any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.
Privacy Guidelines	related guidelines provided to assist in interpreting and implementing this policy and Related Policies, as set out in Appendix 1.
Related Policies	the Company's policies, operating procedures or Processes related to this policy and designed to protect Personal Data, as set out in Appendix 1.
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, genetic data, biometric data, physical or mental health or condition or sexual life. Special category Personal Data can only be Processed under strict conditions and will usually require the express consent of the person concerned.

1. Policy Introduction

1.1. Introduction

- 1.1.1. We Process Personal Data about a range of Data Subjects, such as employees, customers, employees of customers, prospective customers, and suppliers. We Process Personal Data for a number of purposes such as the provision of products and services to our customers as well as employee administration and the management of the Group's businesses. It is critical to Genuit that we are able to use Personal Data in this way. In order to continue to be able to do so, we must comply with the relevant Data Protection Laws.

1.2. Policy on Personal Data

- 1.2.1. We endeavour to ensure that Personal Data is Processed in accordance with the Data Protection Laws and in particular the Data Protection Principles as outlined in paragraph 2.
- 1.2.2. We have put in place systems of work and procedures to ensure that we comply with the Data Protection Laws. We aim to provide all employees with sufficient information, instruction and training as is necessary in order to identify Personal Data and Process it appropriately.
- 1.2.3. This policy will be reviewed at regular intervals and revised where it is considered appropriate to do so, having regard to legislative change, codes of practice, guidance from the ICO, good data protection practice and case law.

1.2.4. Please contact the Company Secretary, the Group's HR Director or your local HR teams with any questions about the operation of this policy, the Data Protection Laws, or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the Company Secretary in the following circumstances:

- a) if you are unsure of the lawful basis on which you are relying to Process Personal Data (see paragraph 5.5);
- b) if you are unsure about the retention period for the Personal Data being Processed (see paragraph 9.8.4);
- c) if you are unsure about what security or other measures you need to implement to protect Personal Data (see paragraph 9);
- d) if there has been a Personal Data Breach (see paragraph 13.2);
- e) if you need assistance dealing with a Data Subject Access Request (see paragraph 14);
- f) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see paragraph 10.3) or plan to use Personal Data for purposes others than what it was collected for; or
- g) if you need help complying with applicable law when carrying out direct marketing activities (see paragraph 9.5).

1.2.5 Please refer to the Company Secretary for further guidance on the completion of contracts to ensure compliance with the Data Protection Laws, or any other area in relation to contract requirements before sharing Personal Data with any third party.

2. Legal obligations on Processing – Data Protection Principles

2.1. If we Process Personal Data we must do so in accordance with the six Data Protection Principles. These state that Personal Data must be:

- 2.1.1. Processed lawfully, fairly and transparently;
- 2.1.2. obtained for a specified and lawful purpose and Processed compatibly with that purpose;
- 2.1.3. adequate, relevant and necessary for the purpose for which it is Processed;
- 2.1.4. accurate and up to date;
- 2.1.5. kept in a form that identifies the Data Subjects for no longer than necessary; and
- 2.1.6. Processed in a manner that ensures its appropriate security.

3. Notification

3.1. Unless an organisation is exempt, it must notify the ICO if it Processes Personal Data. Genuit Group and its trading subsidiaries that are required to do so are currently registered as Data Controllers with the ICO.

- 3.2. We are obliged to ensure that the notification is accurate and up to date at all times. Should any of the details provided as part of the relevant notification change, these must be notified to the ICO. Each Business Unit Managing Director is responsible for ensuring that the notification for their business is kept up to date. Any queries or concerns regarding this should be addressed to the Company Secretary.
- 3.3. Failure to notify the ICO could result in a criminal offence being committed by us or a person who has a duty to notify changes to the ICO.

4. Data Protection Best Practice

- 4.1. We must Process Personal Data in accordance with the Data Protection Laws. We are responsible for:
 - 4.1.1. explaining to all relevant employees the importance of data protection;
 - 4.1.2. providing employees with adequate training, information, instruction and supervision to ensure Personal Data is Processed in accordance with the Data Protection Laws;
 - 4.1.3. assuming overall responsibility for compliance with the Data Protection Laws;
 - 4.1.4. selecting someone to be responsible for ensuring compliance with the Data Protection Laws and making this person known to staff. This person is the Managing Director of the relevant Business Unit, with the relevant HR Director acting as his/her deputy for this purpose;
 - 4.1.5. maintaining a record of how Personal Data is kept and Processed and notifying the ICO in accordance with the Data Protection Laws;
 - 4.1.6. maintaining a record of any breaches of our obligations under the Data Protection Laws and, where necessary, notifying the ICO and, where applicable, the Data Subjects of any such breaches.
- 4.2. We must:
 - 4.2.1. be aware of the issues regarding data protection;
 - 4.2.2. consider the rights of Data Subjects who may be affected by our Data Processing actions;
 - 4.2.3. Process Personal Data in accordance with this policy;
 - 4.2.4. report any Data Subject Access Requests or other questions regarding data protection to the relevant HR Manager; and
 - 4.2.5. report any actual or suspected breach of this policy to the Company Secretary immediately.

5. Processing Personal Data

- 5.1. All Personal Data should be Processed in accordance with the Data Protection Laws, Genuit Group's Privacy Policy and this policy.
- 5.2. Personal Data includes employee data, supplier data, customer data and prospect data. It will not include data relating to a company or organisation, although any data relating to individuals within companies or organisations will be covered.

- 5.3. Examples of Personal Data are employee details including employment records, (see paragraph 15 - Employee Personal Data), any third-party data, for example information relating to a supplier and any information Processed by us in relation to the employees of our customers, and, on occasion, about our own employees in respect of whom our trusted third-party legal advisors provide legal advice. Recorded telephone conversations, notes of legal advice given by our trusted third-party legal advisors relating to a specific individual as well as photographs taken of staff or CCTV images are all Personal Data.
- 5.4. We will Process Personal Data when we obtain, record or hold the information or data or carry out any operation with the Personal Data. The definition of Processing is very broad and will capture almost anything that is done with Personal Data. The following arrangements are likely to involve data Processing:
- 5.4.1. provision of payroll services;
 - 5.4.2. database management;
 - 5.4.3. use of employees' own social media account if related to work issues;
 - 5.4.4. use of employees' own tablet, laptop, smart phone, mobile phone or digital camera to carry out work;
 - 5.4.5. the disposal of old computer or office equipment;
 - 5.4.6. scanning of HR records;
 - 5.4.7. office relocation activities; and
 - 5.4.8. disposal of confidential waste.
- 5.5. We must assume that whatever we do with Personal Data will be considered Processing. To Process Personal Data lawfully we must have a lawful basis for the Processing. There are six lawful bases recognised in law which are as follows:
- 5.5.1. **Consent** - A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.
- Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.
- Unless we can rely on another legal basis of Processing, explicit Consent is usually required for Processing Special Category Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require explicit Consent) to Process most types of Special Category Personal Data. Where Explicit Consent is required, you must issue the Fair Processing Notice to the Data Subject to capture explicit Consent.

Evidence of Consent needs to be captured and records kept of all Consents so that the Company can demonstrate compliance with Consent requirements.

Official guidance states that Consent should only be sought if there are no other, more appropriate, lawful bases for Processing the Personal Data in question.

- 5.5.2. **Legal obligations** – where we are under a legal obligation to undertake the Processing, for example, where we are required to confirm the identity of our employees for right to work checks.
- 5.5.3. **Contractual obligations** – where we have an obligation under a contract with the Data Subject and we must Process the Personal Data to comply with that obligation, for example, under a contract of employment.
- 5.5.4. **Legitimate interest** – where we have a legitimate interest in Processing the data and the legitimate interest does not have a materially adverse impact on the Data Subject's rights. Where we are relying on legitimate interest we should prepare, and regularly review, a legitimate interest assessment to ensure we have ensured the Data Subject's rights are not being materially adversely impacted by the Processing, and we must always give the Data Subject the right to object to the Processing.
- 5.5.5. **Public task** – where the Processing is being undertaken pursuant to a specific task that has been dictated in law. It is highly unlikely this will ever apply to the Group.
- 5.5.6. **Vital interests** – where the Processing needs to be undertaken to protect the vital interests of the Data Subject and there is no other lawful basis that can be used. This should only ever be used in an emergency where there is grave risk to the health and wellbeing of the Data Subject.
- 5.6. The lawful basis that is being used to Process the Data must be recorded and reviewed on a regular basis.
- 5.7. If paragraph 5.6 is not satisfied, you must contact the Company Secretary before Processing the Personal Data to ensure that the Group can legally carry out the proposed Processing activity.
- 5.8. Transparency (notifying Data Subjects)
 - 5.8.1. the Data Protection Laws requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.
 - 5.8.2. Whenever we collect Personal Data directly from Data Subjects, including for HR or employment purposes, we must provide the Data Subject with information about how and why we will use, Process, disclose, protect and retain that Personal Data through a Fair Processing Notice, which must be presented when the Data Subject first provides the Personal Data.
 - 5.8.3. When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required as soon as possible after collecting/receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the Data Protection Laws and on a basis which reflects our proposed Processing of that Personal Data.

6. Information, Instruction and Supervision

- 6.1. Data protection advice for our employees is available from the Company Secretary who will arrange for advice from external advisers if necessary.
- 6.2. We recognise that our employees are a key factor in ensuring we comply with Data Protection Laws and good practice. We are committed to ensuring they receive training and development to help fulfil our legal and good practice obligations regarding the Processing of Personal Data.
- 6.3. Employees should only Process Personal Data where they have received adequate training to do so. We will ensure that all new employees, particularly those with access to Personal Data, are trained on this policy as soon as possible after they are recruited. Please also see paragraph 7 (Training and audit).
- 6.4. If any employee feels that they need additional training they should contact their HR Manager who will arrange for additional training to be provided.
- 6.5. If any employee considers that any task or work they have been asked to undertake involves the Processing of Personal Data and are unsure whether or not the task or work would be in breach of Data Protection Laws, this should be discussed in the first instance with their HR Manager who will be able to provide guidance and advice as to what to do.

7. Training and audit

- 7.1. We are required to ensure all employees have undergone adequate training to enable them to comply with Data Protection Laws. Where you are scheduled to attend training you must do so, and your attendance will be monitored and logged.
- 7.2. We must regularly review all the systems and Processes under our control to ensure they comply with this policy and check that adequate governance controls and resources are in place regarding the proper use and protection of Personal Data. We must also regularly test our systems and Processes to assess compliance.
- 7.3. This policy will be updated as required, following any changes in the law, or at a minimum, every two years. Responsibility for issuing new versions of this policy sits with the Company Secretary. All employees will be required to confirm that they have read and understood the updated policy's contents and attend mandatory training as required. This confirmation will be retained by HR.

8. Monitoring the Use of Personal Data

- 8.1. You must keep and maintain accurate corporate records reflecting our Processing, including records of Data Subjects' Consents, procedures for obtaining Consents, and legitimate interest assessments in accordance with the Company's record keeping guidelines.
- 8.2. These records should include, at a minimum, the name and contact details of the Data Controller, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

- 8.3. We are committed to ensuring this policy is put into practice and that appropriate working practices are being followed. To this end, the following steps will be taken:
- 8.3.1. all Company Personnel who deal with Personal Data will be made aware of data protection issues and encouraged to work towards continuous improvement in the way we Process Personal Data;
 - 8.3.2. Company Personnel will be provided with the tools and resources they require to assist them in the Processing of Personal Data in accordance with this policy, and the Data Protection Laws;
 - 8.3.3. spot checks may be carried out by managers on employees who handle Personal Data on a regular basis or who Process sensitive or other confidential Personal Data to ensure they are complying with this policy, the Data Protection Laws, and that they are using systems and procedures as expected and required.
 - 8.3.4. Complaints on our data protection practices may be received from; employees, potential employees who have applied for roles within the Group, ex-employees, suppliers, customers, employees of our customers, or others whose Personal Data we handle.
- 8.4. The Company Secretary will be responsible for investigating any complaints about our data protection practices and for arranging for any identified improvements to be implemented to prevent recurrences of such complaints.
- 8.5. Where we engage in a new way of Processing Personal Data, we shall review that new method and ensure that any Personal Data Processed is done in accordance with the law and good practice. This is likely to involve the preparation of a Data Protection Impact Assessment (DPIA) which may require input from external advisors and, in certain circumstances, the ICO.

9. Handling and Storing Personal Data and Data Security

9.1. We shall:

9.1.1. take appropriate technical and organisational measures to guard against unauthorised or unlawful Processing of Personal Data. The Data Protection Laws require procedures and technologies to be implemented to maintain the security of all Personal Data from the point of collection to the point of destruction. Maintaining data security means guaranteeing the confidentiality, integrity and availability of the Personal Data, defined as follows:

9.1.1.1. “Confidentiality” means that only people who are authorised to use the Personal Data can access it;

9.1.1.2. “Integrity” means that Personal Data should be accurate and suitable for the purpose of which it is Processed; and

9.1.1.3. “Availability” means that authorised users should be able to access the Personal Data if they need it for authorised purposes. Personal Data should therefore only be saved on the Group’s network instead of individual PCs, laptops or smart phones.

9.1.2. ensure that employees who handle Personal Data are adequately trained and monitored;

9.1.3. ensure that passwords and physical security measures are in place to guard against unauthorised disclosures. Please refer to the IT User Policy; and

9.1.4. where employees are allowed to work from home or use their own device for work, employees must ensure they comply with the appropriate policies in respect of such activities.

9.2. Paper Records

9.2.1. Manual data refers to paper and other non-digital Personal Data, records (such as copies of photographs or plans) which are recorded as part of a relevant filing system or with the intention that it should form part of such a system.

9.2.2. A relevant filing system is any set of information relating to individuals which is structured either by reference to individuals or by reference to criteria relating to individuals in such a way that specific information relating to a particular individual is readily accessible. You should treat all Personal Data, however stored or held, in accordance with the principles set out in the Data Protection Laws.

9.2.3. We shall ensure that all written records containing Personal Data shall be reviewed in accordance with paragraph 9.2.5 and a record shall be kept of all such reviews.

9.2.4. Genuit Group also strives to minimise its use of paper records and operates a ‘clean desk’ policy to minimise the amount of paper that is being used and stored.

9.2.5. Manual records containing Personal Data must be reviewed in order to ensure that the data contained within them is accurate, not excessive, up to date and adequate for their purpose. Where possible, manual records should be replaced by digital files as and when they are periodically reviewed or retrieved for whatever purpose.

9.2.6. Any documents containing Personal Data or Special Category Personal Data should not be left on a desk on view when the desk is unattended.

- 9.2.7. Any documents containing Special Category Personal Data must be stored securely and in such a way that only those who need to access it have access (for example, in locked filing cabinets).

9.3. Privacy by design and DPIAs

- 9.3.1. We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with Data Privacy principles.
- 9.3.2. We must assess what Privacy by Design measures can be implemented on all programs/systems/Processes that Process Personal Data by taking into account the following:
- a) the state of the art;
 - b) the cost of implementation;
 - c) the nature, scope, context and purposes of Processing; and
 - d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Data Controllers must also conduct DPIAs in respect to high-risk Processing.

- 9.4. You should contact the Company Secretary, Group HR Director or your line manager when implementing major system or business change programs involving the Processing of Personal Data including:
- a) use of new technologies (programs, systems or Processes), or changing technologies (programs, systems or Processes);
 - b) Automated Processing including profiling and ADM;
 - c) large scale Processing of Special Category Personal Data; and
 - d) large scale, systematic monitoring of a publicly accessible area.

so that an appropriate DPIA assessment can be carried out. If requested, you must provide such support as is needed to assist in the completion of any DPIA.

9.5. Direct marketing

- 9.5.1. We are subject to certain rules and privacy laws when marketing to our customers. For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale or potential sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.
- 9.5.2. The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information. Best practice is to have an 'unsubscribe' option at the foot of all such communications which, when selected, allows the Data Subject to easily communicate their desire for us to cease communicating with them in this manner.

- 9.5.3. A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

9.6. Special Category Personal Data

9.6.1. We must:

- 9.6.1.1. only collect Special Category Personal Data where it is absolutely required and, even then, to the minimum extent necessary for the purpose for which it is required;
- 9.6.1.2. take particular care of Special Category Personal Data and, where we have access to such information, we must make sure we Process it properly and in accordance with the Data Protection Laws;
- 9.6.1.3. unless the Special Category Personal Data is being Processed in an emergency, we must make sure we obtain the explicit Consent of an individual before Processing Special Category Personal Data relating to them; and
- 9.6.1.4. store all Special Category Personal Data with adequate security measures to prevent unauthorised disclosure. Such measures should include lockable cabinets and password protection and encryption of automated data.

9.7. Technical Security measures

- 9.7.1. We will ensure that all computers have protection against malicious software/viruses and that software is not installed and information is not downloaded without first being checked for viruses and other malware. We will keep up to date with patches, fixes and new releases to ensure that our systems are protected against known security issues. Please refer to the IT Policy.
- 9.7.2. We must always store Personal Data electronically on our central computer system, rather than on local drives, devices or at home.
- 9.7.3. All computers and documents containing Personal Data should be password protected and all passwords should be kept secret at all times. Employee passwords should include a mixture of letters, capital letters, numbers and special characters (such as !?#*&) and not be easy to guess or use common combinations - such as "1234". As per the password policy in the IT User Policy.
- 9.7.4. We must store devices containing Personal Data carefully if taken out of the work place. Laptops, tablets, smart phones and other mobile devices should be stored securely and not left unattended in cars or in public places or on top of desks or table tops at home left unattended overnight.
- 9.7.5. We must not use personal computers for work purposes unless this has first been cleared with Group IT department.
- 9.7.6. We must ensure that individual monitors are positioned so they do not show confidential information to passers-by. This is particularly important if employee PC displays employee data or Special Category Sensitive Data. PCs should be logged off when left unattended. We can provide covers for screens that stop others from seeing what is on the screen unless looking directly at the screen from the correct angle.

9.8. Organisational Security Measures

9.8.1. Manual records

Any manual records that are essential must be kept secure by the use of locked cabinets. Access to such records should be restricted to those employees whose job requires access. Where a manual record is in constant use we must take appropriate security measures. You should operate a 'clean desk' policy, removing bins from the office space and replacing them with confidential paper disposal areas and ensure all computers are locked when not in use.

9.8.2. Telephone enquiries

When we deal with telephone enquiries we must be careful about disclosing any Personal Data held by us. In particular we must:

- 9.8.2.1. check the caller's identity to make sure that information is only given to a person who is entitled to it;
- 9.8.2.2. suggest that the caller puts their request in writing, where you cannot be sure about the caller's identity or where their identity cannot be checked; and
- 9.8.2.3. refer to your HR Manager for assistance in difficult situations.

9.8.3. Building access

Building access codes must be kept secret. If access to a building is by fob, or similar technology, you must never allow anyone else to use your fob to gain access to the building. Where security passes are in place we will take measures to ensure that all staff wear such passes in a prominent, visible position. Any stranger seen in entry-controlled areas should be reported immediately to your site reception or, if appropriate, security.

9.8.4. Deletion or destruction of data

The Company maintains retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. Where Personal Data needs to be deleted or destroyed, adequate measures should be taken to ensure that such data is properly and securely disposed of. Personal Data must be destroyed in accordance with the Company's Data Retention and Destruction Policy. You must take all reasonable steps to destroy or erase all Personal Data that is longer required in accordance with all the Company's Data Retention and Destruction Policy. This includes requiring third parties to delete such data where applicable. This will include the destruction of files and back up files and the physical destruction of manual files. The sale or destruction of IT equipment including PCs, laptops, smart phones and other mobile devices should be treated as a data Processing activity.

9.9. Policy update

All security policies and procedures must be regularly monitored and reviewed to ensure that Personal Data is being kept securely. Policies and procedures shall be reviewed against good data protection practice including ICO guidance and case law. Where policies and procedures are found to be inadequate, prompt and appropriate action shall be taken in order to rectify such inadequacies. This shall include a review of the security sections and the consideration and implementation of replacement provisions to rectify such inadequacies.

10. Transfers to Third-Parties

- 10.1. Sometimes there will be a need to transfer Personal Data to a third-party (i.e. someone, or a company, that is not part of the Genuit Group). For example, this could include transferring payroll data to a third-party payroll provider or transferring marketing lists to a marketing agency for the purposes of running a marketing campaign.

- 10.2. Prior to any Personal Data being transferred to a third-party we must ensure that we have a contract in place with that third-party that contains contractual provisions that safeguard the Personal Data being transferred and that complies with the requirements of the Data Protection Laws.
- 10.3. If required there is a template Data Processing Impact Agreement that should be used for this purpose which can be obtained from the Company Secretary.

11. International Transfers

- 11.1. As Genuit Group is a multi-national business, there are occasions when Personal Data will be transferred internationally.
- 11.2. Where Genuit transfer's any Personal Data that falls within the scope of the Data Protection Laws outside of the EEA then it will only do so where:
 - 1) It has satisfied itself that the recipient has suitable safeguards in place to protect the data and ensure it is Processed in accordance with the Data Protection Laws; and
 - 2) There is a written contract in place between the Genuit Group subsidiary and the third-party that contractually binds the third-party to Process the data in accordance with the Data Protection Laws.
- 11.3. If required there is a template Data Processing Agreement that should be used for this purpose which can be obtained from the Company Secretary.

12. Data Subject's Rights

- 12.1. Under the Data Protection Laws all Data Subjects have a number of rights with regard to their Personal Data, namely:
 - a) The right to be informed – this is the right for all Data Subjects to be told what Personal Data is collected and how it is used. Genuit Group's Privacy Policy together with the Data Retention and Destruction Policy fulfil this requirement.
 - b) The right of access – this is the right for a Data Subject to require the Data Controller to provide them with a copy of the Personal Data they hold relating to them. This is known as a 'Subject Access Request'. We have a specific Data Subject Access Request Policy which covers everything you need in relation to Subject Access Requests.
 - c) The right to rectification – this is the right for a Data Subject to require a Data Controller to correct any inaccurate information they may hold.
 - d) The right to erasure – this is the right for a Data Subject to require a Data Controller to delete the information they hold about them.
 - e) The right to restrict Processing – this is the right for a Data Subject to require a Data Controller to stop undertaking certain Processing activities.
 - f) The right to portability – this is the right for a Data Subject to require that the Data Controller provide a copy of their Personal Data to a third party in a format that is readable to that third party.
 - g) The right to object – this is the right for a Data Subject to object to the Data Controller's use of their Personal Data for specific purposes such as marketing.

- h) The right to object to automated decision making – this is the right for a Data Subject to require that a decision made by automated means to be reviewed by a human being.

The Data Subject rights are not absolute and the ability to exercise a right is dependent on the purpose for which the data was collected and the lawful basis under which it is being used. For example, if Personal Data is being collected pursuant to a legal obligation (i.e. for reporting for taxation purposes) then the Data Subject does not have the right to have that data deleted.

The table below outlines what rights can be exercised depending on the lawful basis under which the Personal Data in question was obtained.

	Right to Access	Right to Correction	Right to Erasure	Right to Restrict Processing	Right to Object	Right to Transfer	Right to Withdraw Consent
Consent	✓	✓	✓	✓		✓	✓
Contractual Obligation	✓	✓		✓		✓	
Legal Obligation	✓	✓		✓			
Vital Interests	✓	✓		✓			
Public Task	✓	✓		✓			
Legitimate Interests	✓	✓	✓	✓	✓		✓

Full information about the rights of the Data Subject and how and when they can be exercised can be found on the ICO's website.

13. Security Breach, Notification and Reporting

13.1. Introduction

We shall ensure that Personal Data is stored and used in accordance with this policy and the Data Protection Laws. However, breaches may occur despite our best efforts. It is therefore essential that on discovering a breach has occurred, the breach is reported in accordance with Genuit Group's Data Breach Management Policy to ensure that the impact of the breach on Data Subjects is minimised and our liability for the breach can be limited as much as possible. Reporting and thorough investigation of incidents also helps to ensure that potential risks and problems are identified early and appropriate changes are made to minimise the possibility of future data protection breaches occurring.

13.2. What is a data security breach?

13.2.1. The sixth data protection principle provides that Personal Data must be Processed in a manner that ensures its appropriate security.

13.2.2. A data security breach is any situation or happening that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

13.2.3. The most common data security breach is the release (no matter how caused) of Personal Data to a third party who is not authorised to view, hold or otherwise Process the information. Examples of breaches would be:

13.2.3.1. an employee leaving a piece of Personal Data about another employee or the employee of a customer (such as their address, date of birth etc.) on a desk when the employee leaves the desk so that other employees who do not have permission to view the information can see it;

13.2.3.2. the sending of an e-mail containing Personal Data (for example a database) to a third party that is not entitled to see it, for example, by entering the wrong email address;

13.2.3.3. the loss of a folder of papers or an electronic device such as a memory stick containing Personal Data in a public place;

13.2.3.4. the theft of a laptop, tablet, smart phone, mobile or digital device (such as a camera) containing Personal Data, such as a database or e-mails;

13.2.3.5. the premature deletion or destruction of Personal Data that should have been retained in accordance with our Data Retention and Destruction Policy.

13.3. Who can report breaches?

13.3.1. Data security incidents can be reported by Genuit Group and its subsidiaries, an employee, a potential employee who has applied for a role within the Group, ex-employees, a customer, an employee of a customer, a supplier; or a member of the public.

13.4. No matter the cause of a data breach it must be reported without any delay. If you become aware of a data breach, or a potential data breach, you must notify your HR Manager immediately, who will then liaise with the Company Secretary.

13.5. Under the Data Protection Laws we have no more than 72 hours to report a breach after becoming aware of it, or after we ought to have become aware of it. If you are aware of a breach, or a potential breach, and fail to report it as required above it exposes us to potential investigations, fines and criminal convictions. A failure to report a breach, or potential breach, is a disciplinary offence.

14. Dealing with Subject Access Requests

14.1. What is a Subject Access Request?

14.1.1. Data Subjects have a right of access to a copy of their Personal Data.

14.1.2. A Subject Access Request is any request from a Data Subject which indicates that the person wants to know what information is kept about them.

14.1.3. A Subject Access Request can be made in any form, including verbally, so all Company Personnel must be conscious of the risk of a Subject Access Request being made and missed.

- 14.1.4. If a verbal request for information is received we will ask the Data Subject to put the request in writing by completing the Subject Access Request Form, in accordance with Genuit Group's Data Subject Access Request Policy to ensure that we respond to it accurately and in a timely manner.
- 14.1.5. All Data Subject Access Requests will be dealt with in accordance with Genuit Group's Data Subject Access Request Policy.
- 14.2. The Group's Data Subject Access Request Policy provides further information on how we require Subject Access Requests to be handled.

15. Employee Personal Data

- 15.1. The lawful bases Genuit relies on for collecting and Processing employee data are:
 - 15.1.1. Legal obligation, as Genuit has legal obligations as an employer to collect Personal Data relating to its employees;
 - 15.1.2. Contractual obligation, as Genuit has contracts of employment with each employee which includes obligations that require Genuit Process the Personal Data of its employees; and
 - 15.1.3. Legitimate interest, as Genuit may over time Process Personal Data relating to its employees for its own and their benefit, where such Processing falls outside the scope of legal obligation and contractual obligation and does not negatively harm the employees' rights.
- 15.2. In the course of recruitment and employment we will collect, retain and Process information consisting of Personal Data including Special Category Personal Data about employees. Employee data will be Processed in accordance with our Fair Processing Notice.
- 15.3. All employment records, including application forms, interview notes, sickness notes, annual leave records, promotion and appraisal notes, training records, disciplinary and dismissal notes and reports, references (whether confidential or otherwise and whether given or received) and general personnel file notes must be Processed in accordance with the Data Protection Laws.
- 15.4. HR records and all written information regarding an employee, including appraisal, career progression and discussions regarding salary should be set out in a manner which contemplates that it may be disclosable as Personal Data. All records should therefore be clear and fair and where opinions are expressed these should be shown to be such.
- 15.5. The information we hold for the above purposes will be retained for the duration of an employee's employment. The purposes for which we hold any information about the employee after the end of employment are for use solely for any residual employment related matters including (but not limited to) the provision of job references, Processing applications for re-employment, matters relating to pre-termination and retirement benefits and allowing us to fulfil contractual or statutory obligations.
- 15.6. Where employee records are maintained for organisational analysis, we will take care to ensure that only Personal Data is kept which is necessary to satisfy the purpose for which it is kept. Where possible, such data should be anonymised.
- 15.7. All disciplinary actions, commentary, reports and any reports relating to a dismissal of an individual shall be written in a manner which is fair and accurate.
- 15.8. All employee records shall be regularly reviewed to ensure that they are accurate, not excessive, up to date and adequate for their purpose.

15.9. Use of Personal Data in recruitment

- 15.9.1. All recruitment advertisements must contain information which enables applicants to identify that they are applying to us.
- 15.9.2. The interview notes of all applications should be written giving consideration to the fact that these will amount to Personal Data under Data Protection Laws. All interview notes should therefore be a fair and accurate representation of the interview. Any opinions expressed should be included in a manner which contemplates that they may be disclosable at a later date.
- 15.9.3. Where an individual candidate is interviewed but we wish to offer the individual employment other than in the post which the individual has applied for, care must be taken to ensure that the individual has consented to their Personal Data being used for this purpose. Candidate details must not be shared with other organisations unless specific permission has been obtained from the candidate to so do.
- 15.9.4. Any decision to shortlist candidates, where such decision making is made in writing, should be done in a manner which is fair and lawful.

16. Customer, Supplier and Prospect Data (“Trading Data”)

- 16.1. The lawful bases Genuit Group relies on for collecting and Processing Trading Data are:
 - 16.1.1. Contractual obligation, as Genuit’s contracts with customers and suppliers are likely to require Genuit to undertake some Processing to enable us to fulfil and/or enforce our contractual obligations; and
 - 16.1.2. Legitimate interest, as Genuit has a legitimate interest in Processing this data to further its business purposes and such Processing is what the Data Subjects would ordinarily expect to take place and does not negatively affect their rights.
- 16.2. Much of our Trading Data has the potential to be, and data that relates to the employees of our customers is most likely, Personal Data covered by the Data Protection Laws.
- 16.3. All records relating to Trading Data which contain Personal Data, including (but not limited to) employment records, must be Processed in accordance with Data Protection Laws and this policy.

17. Who to speak to about data protection

- 17.1. If you have any questions or concerns about the way that Genuit is handling any Personal Data, whether about you or anyone else, please contact your HR Manager in the first instance. If HR are unavailable please email company.secretary@genuitgroup.com who will be able to help.

18. Changes to this policy

- 18.1. We reserve the right to change this policy at any time and will notify you accordingly.
- 18.2. This policy does not override any applicable national data privacy laws and regulations in countries where the Group operates.

APPENDIX 1

RELATED POLICIES, PROCEDURES AND DOCUMENTS

- Group Policies and procedures handbook
- Fair Processing Notice – Employee Data
- Privacy Policy (available at www.genuitgroup.com)
- Data Retention and Destruction Policy
- Data Breach Management Policy
- Data Subject Access Request Policy
- Clean Desk Policy
- Information Security Policy
- Data Privacy Impact Assessment template

APPENDIX 2



DATA PROTECTION POLICY COMPLIANCE DECLARATION

I confirm that I, _____ have read the Data Protection Policy, version ____ on
__/__/____ and understand my obligations when Processing Personal Data on behalf of Genuit Group
and its subsidiaries and confirm that I have attended and completed the training on its requirements.

Business Unit: _____

Signed: _____

Date: _____