DATA PROTECTION AND DATA SECURITY CORPORATE POLICY

Purpose

1. This document defines the REEID GCE policy on data protection and data security and is based on the following principles:

- The REEID GCE will comply with all relevant legislation, particularly the Data Protection Act 1998, and base its policies and practices on compliance with the eight Data Protection principles contained therein.

- Ensuring compliance is a corporate responsibility of the Company requiring the active involvement of, and appreciation by, all staff at all levels of the organisation.

- The Company will strive to ensure best practice with regard to data protection and data security processes and procedures.

- The Company will strive to improve practices and procedures using external guidance, monitoring of jurisprudence in the relevant areas, and adopting examples of best practice elsewhere.

- The Company will provide support and services to enable staff handling personal data to remain compliant with the legislation and the corporate's requirements in respect of data security.

Introduction

2. At REEID GCE, personal data are held about customers, staff, and the public. The Company needs to hold information about its customers and staff for reasons which include, but are by no means limited to, the following:

- Archiving financial records

- Archiving projects records

Data may also be held on other individuals, such as candidates, visitors to the Company, suppliers, employees of other organisations who are involved in our projects.

The Data Protection Act 1998 (DPA) places responsibilities and obligations on organisations which process data about living individuals. It also gives legal rights to individuals in respect of personal data held about them by others. The DPA may be found on the internet at https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

3. REEID GCE is required to have policies and procedures in place to ensure compliance with its obligations under the Act that extend across its customers, staff, and the activities of the company.

4. Scope

This policy applies to:

- Company Customers
- All staff employed by the company.
- Any non-company staff with any degree of access and/or use of personal data held by the company.
- All corporate activities that involve the processing of personal data as defined by the Data Protection Act 1998.

5. Definitions

The following definitions apply to this policy:

- The Act: Data Protection Act (DPA) 1998.
- Data security breach: Any occurrence of any unauthorised or unlawful processing of personal data held by REEID GCE, or the accidental loss, destruction of or damage to any such personal data.
- Data subject: A living individual who is the subject of personal data.
- Data controller: A person or organisation which controls the purposes and manner in which data are processed. REEID GCE is a data controller, and the point of contact is the Management Office.
- Data processor: Any person or persons that process information on behalf of a data controller.
- Data: All information in digital format, or manual data within a 'relevant filing system'.
- The Information Commissioner (ICO): The supervisory authority, reporting directly to Parliament, that enforces and oversees the DPA, and other information related legislation. The ICO maintains a public register of data controllers. The process of adding an entry to the register is called notification. The Company's notification covers the classes of data which are processed and is updated from time to time.
- Information life cycle: The time span that information processed by REEID GCE remains 'live' and relevant to the Company (inclusive of its disposal or destruction) and for which the Company has obligations under this, or any other policy.

- Personal data: Data which relate to a living and identifiable individual, including computerised data and some manual data (i.e. paper-based records, microfiche, etc.). When the DPA was first passed into law, it covered data held in a "relevant filing system", which is defined in the DPA as a "set of

information" 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". However, the Freedom of Information Act 2000 (FOIA) modifies and extends the DPA to apply to "unstructured personal data". Unstructured personal data are any personal data which fall outside the definition of the relevant filing system given above. The difference may be illustrated as follows. Personnel records are clearly part of a "structured filing system" as they are arranged by surname or employee number. However, a member of staff may serve on a Company committee, and that person's name will appear in the minutes of that committee. The minutes are not structured by names, but by the dates of committee meetings. Under the modification to the DPA, such data now fall within its remit.

- Processing: An action of any sort taken in regards personal data during the lifecycle of that personal data. This will include but is not limited to, obtaining, storing, adapting, transferring, transmitting, disposal and destruction.

- Relevant filing system: Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set 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.

- Sensitive personal data: The DPA recognises that certain types of personal data should be treated with regard. Such data include racial or ethnic origin; political opinions; religious beliefs; membership of a trade union; physical or mental health or condition; sexual life; and criminal offences.

- Subject Access Request (SAR): The means by which any individual exercises the right, pursuant to section 7 of the DPA any individual to see a copy of the information an organisation

holds about them. A SAR can include the following elements:

- a request to be told whether any personal data is being processed.

- a request to be given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;

- a request to be given a copy of the information comprising the data; and

- a request to be given details of the source of the data (where this is available).

6. Aims

The aims of the Data Protection and Data Security Policy are to:

- Set out the obligations of the Company with regard to data protection and data security.
- Establish the guiding principles for the Corporate's actions in this area.
- Provide a policy framework to ensure local compliance with the DPA and the Corporate's requirements in respect of data security.

Policy statements Notification

7. REEID GCE will comply with the notification obligations placed upon it by the Act and associated regulations; specifically renewing notification with the ICO yearly and ensuring that the notification is current and accurate. To further the latter, the Company will conduct a comprehensive review of its notification no later than every 5 years, and more frequently should the activities or data holdings of the Company so demand.

Personal data held by REEID GCE

- Data are collected at new Customer registration process
- Data are also added subsequently to client's records, for example:

changes of address. Change of name or title, or position

- Changes of tax ID so adjacent personal record
- Human Resource collects data on staff and creates a personnel file for every member of Company staff. Some of this information will also be held by individual administrative departments within the company business units. Such data will include:
- applications for job at REEID GCE
- terms of appointment
- appraisal
- promotions
- leave records

8. All staff should ensure that any information that they provide to the Company in connection with their employment is accurate and up-to-date. REEID GCE has ultimate responsibility for ensuring the personal information it holds is accurate and up to date.

Processing obligations - general

Data Protection principles in general

9. Under the DPA, personal data must be processed in accordance with the following eight Data Protection Principles. These principles are contained within Schedule 1 of the Act and are the fundamental obligations imposed by the Act with regard to the processing of personal data. The term processing has a wide application which includes the mere fact of holding data about a living individual, as well as the alteration, disclosure and destruction of personal information. The eight Data Protection Principles state that data must:

1. be obtained and processed fairly and lawfully and only if certain conditions are met;

2. be obtained for specified and lawful purposes;

3. be adequate, relevant and not excessive for those purposes;

4. be accurate and up-to-date;

5. not be kept for longer than is necessary;

6. be processed in accordance with the rights of data subjects;

7. be kept safe from unauthorised access, loss or destruction; and

8. not be transferred to countries outside the European Economic Area (EEA), unless to countries with equivalent levels of data protection.

The first principle - fair processing

10. The requirement for 'fair processing' is set out in the first data protection principle and is the most important principle with regard to the processing of personal data. In essence, this principle demands, and it is the Company's policy that, all personal data for which the Company is the data controller, will be processed in line with the expectations of the relevant data subjects, and that all data subjects will have adequate notice of any processing undertaken by the Corporate.

- If any professional services area is planning to collect personal data from anyone, consent to store and handle the information must be obtained from the individual at the time of the data collection. Advice on writing the appropriate privacy notices is available from the Company Secretary.

- When a Customer registers he or she is issued with a data protection notice. The notice sets out the types of data which are being collected and the uses to which these will be put, including transfers to other directly related to REEID GCE organisations. It also informs the Customer that, by signing the

registration form, he or she consents to the processing of those data, for purposes connected with the legitimate activities of the Corporate.

- For staff, a data protection notice is included on application forms for employment at REEID GCE which sets out the data which are collected, the uses to which they will be put, and seeks consent for their processing. There is also a notice for successful applicants when they join the Corporate.

- Particular attention is drawn to the collection of data on ethnic origin, disability and other protected characteristics, since these are among the types of sensitive data defined in the DPA. Explicit consent must be obtained for the processing of sensitive data, and this is made clear in the notices issued to staff and customers, which explain that, by providing these data, the staff member or customer consents to the processing of his or her data within carefully-defined limits. An individual cannot be forced to provide these data, and he or she is at liberty to refuse to provide them on the application or registration form (which means, effectively, that consent for their processing has been withheld).

The seventh principle - data security

11. Adequate data security is essential to meet the requirements of the seventh Data Protection

principle. Where anyone subject to this policy is in possession of personal data they must:

- ensure that the personal data is technically stored and handled in line with approved Company data security policies and processes;

- ensure that corporate measures are in place to guard against unauthorised or unlawful damage or destruction of the personal data. Such measures could include: restricting access to the data to minimum number of persons possible; ensuring that all digital personal data is password protected wherever it may reside; ensuring that any personal data are not left 'in the open' either in paper form, or on a screen in digital form; ensuring that access to the area in which the personal data is stored is restricted to only those persons who need to be there; minimising the need for transfer of the data, if transfer is required; and ensuring that Company data security protocols are in place and observed;

- take steps to provide an adequate level of training in DPA and information security to anyone with access to the personal data, inclusive of anyone outside of the Company that may have access to the data.

Other processing obligations

12. Staff should ensure that personal data are:

- processed only for the purposes for which they were collected (note that simply holding data on file counts as processing);

- not divulged to third parties without the subject's consent;

- relevant, accurate and up to date;

- adequate but not excessive for the stated purpose;
- disposed of as confidential material when they are no longer needed for the purposes for

which they were collected and in line with Company data retention procedures;

- not transferred outside the EEA unless there are adequate measures in place that ensure a level of protection equivalent to that afforded by the Act.

Data sharing

13. Information should not be transferred to third party unless such a transfer is authorised by the Act itself.

14. The Act authorises release to third parties without notice to the data subject under certain limited circumstances such as:

- detection or prevention of crime, apprehension of offenders;
- protection of the vital interests of the data subject;
- pursuant to a contract to which the data subject is a party;
- pursuant to a legal obligation imposed upon the company;
- where necessary for the pursuit of the legitimate interests of the Company or any third party save where such processing is unwarranted by prejudice to the rights, freedoms or legitimate interests of the data subject.

15. Any proposed data sharing that does not meet the above conditions must be reviewed by the Company Unit who has the responsibility of determining whether, on the facts of the case, a data processing agreement is warranted. As a general rule, one-off, ad hoc data sharing events will not require an agreement whilst any on-going data sharing will require such an agreement.

16. If a data processing agreement is warranted, the Company will work with the relevant line manager with operational responsibility for the data sharing to draft and agree an agreement that assures that the Company meets its compliance obligations.

17. Data that is appropriate under the Act to share must be transmitted in the most secure form available. As far as possible data should be transmitted solely over the secure Company network and the transmission of data via paper, post or independent electronic devices is strongly discouraged. REEID GCE IT network is such a secure system, with fully managed access control, backup and recovery processes in place.

23. Where it is legitimate to share personal data with external organisations, the following hierarchy of actions should be adhered to:

- Data should be uploaded via a secure portal wherever possible; most organisations using this method publish details of security systems on their websites.

- Where there is no secure portal, data should be transmitted electronically (for example, as files, databases, PDF files, images) over secure networks. These files should be encrypted and, if so, then email is acceptable for such transmission. Where the transmission of large sets of data is unavoidable, IT Services can advise how this is best achieved.

- Data should be accessed through the host information system directly (if working away from the office, this may be done via a remote connection).

- If it is unavoidable to share paper copies of sensitive data, they should be mailed in securely sealed envelopes and sent by courier or registered post. An individual's personal data in the form of, for example, assessment results or letters of appointments, may be sent in sealed envelopes using normal postal systems.

- Care should be taken when transmitting sensitive data to unfamiliar recipients. Wherever possible the authenticity of the recipient should be checked with a known contact at the recipient organisation.

Specific Company-related processing policies References

24. It is relatively common for staff or Customers to request access to personal references written at the time of their application for employment or signup, or for employment or elsewhere. This is an area where a specific exemption is written into the DPA: references given by REEID GCE (the data controller) are exempt from the subject access provisions. Thus, Customers and staff cannot apply to see references provided by Company and sent to another organisation. They may, however, apply to the organisation to which the reference has been sent.

25. Similarly, they may apply to see references which have been received by the Company and which may be held in (say) a personnel file. These references received by the Company are treated as any other items in a file, and we would follow the normal procedure regarding handling subject access requests by data subjects. It is worth bearing in mind that anonymisation is unlikely to be effective where references are concerned, and it is very likely that the Company would seek the consent of the author before releasing them, before deciding whether or not it was reasonable to release the reference "in all the circumstances".

26. The ICO has advised that, where a reference has had an adverse effect on the subject of the reference, the subject's right of access will normally outweigh any other circumstances, even if the reference was given in confidence, and the author has expressly refused his or her consent to its disclosure.

Research

27. The Act allows certain exemptions in the case of personal data which are collected and processed for research purposes, or for historical or statistical purposes. If the processing is only for the purposes of research (and is not used to support decisions about individuals) then

- the data can be kept indefinitely,

- subject access does not have to be granted, as long as the results of the research are anonymised.

28. This is common in the case of medical research papers which often refer to Ms A, Mr B, et al.

29. Care should be taken if a key is retained which enables anonymised data to be decoded and therefore attributed to individuals. An appropriate level of care would exist if the key was only known to those individuals directly involved in the research, and kept securely, and separate from the usual location of the anonymised data.

System and process assessment

30. Any system, project, process, or information holding within the Company that involves personal data must be compliant with the Company obligations under the Act and an assessment and evaluation of compliance will be necessary.

31. Privacy Impact Assessment - in the case of major systems, a full, or truncated Privacy Impact Assessment may be required. This will only be required in the case of major initiatives involving substantial amount of personal data or particularly sensitive or potentially risky processing of data. The ICO provides brief guidance on this process.

32. A Company generated checklist of data protection compliance should be completed at the commencement of any project or system to identify data protection issues, risks and processes that need to be addressed. The checklist is available from the Management office

33. For other smaller processing issues, advice and guidance will be available from the Management Office. Where such advice and guidance are given, every opportunity will be explored to expand the knowledge and awareness of the individual or organisational unit seeking the advice and guidance.

Training and awareness

34. Training and awareness are essential for Company to be able to meet its obligations under the Act.

35. The Management Department has primary responsibility for ensuring that adequate and appropriate training and awareness exist within the Company, working closely with the Director of Human Resources and the Director of IT Department.

36. All employees, upon obtaining employment with REEID GCE, will receive general information on the Act and the Company obligations thereunder as a component of the induction documentation and process.

37. The Management Office has overarching responsibility for the creation and maintenance of web-based and print material for reference and awareness. This post is also responsible for ensuring that scheduled training is available to staff and providing ad hoc training where appropriate.

38. The Management Office, in conjunction with relevant Company departments, will identify those roles requiring training and awareness of data protection responsibilities and will work with the relevant department to ensure that adequate and appropriate training is provided. Monitoring of the effectiveness of training and awareness activities should be undertaken and maintained consistently.

Data breach management

39. It is the responsibility of all Company staff to avoid data security breaches, but where one does occur, the affected department, or individual must report the breach to the Company Secretary at the earliest possible opportunity.

40. Any personal data breaches will be handled in accordance with current guidance from the ICO and the disciplinary procedure, and investigation of any breach will initially be the responsibility of the Company Secretary or nominee.

41. Any decision regarding the notification of either the ICO or affected parties of any breach will be taken on the authority of the Academic Registrar.

42. The general procedure in the case of a data security breach will follow ICO guidelines and focus on the proper completion of four stages of breach management:

- Containment and recovery
- Assessment of on-going risk
- Notification of breach
- Evaluation and response

43. It is the responsibility of the Company Secretary to ensure that all four stages are addressed. The Management Office is responsible for authorising any actions and signing off that each stage has been successfully undertaken and completed.

Data Subject Access Requests (SAR)

44. Persons about whom REEID GCE holds data (data subjects) may make a Subject Access Request (SAR) to see those data, and to receive or view copies of those data in permanent intelligible form (print-outs or photocopies). Customers, staff or any individuals external to the Company who wish to make a SAR should be directed to the appropriate page of the Company ’s website. The detail of the processes and procedures to be followed in administering a SAR are set out in the Data Protection SAR Procedure available from the Company Secretary.

Data storage, retention and disposal

45. Adequate data security is essential to meet the seventh principle of the Act and the following safeguards are in place at an organisational level:

- Each of the corporate systems at REEID GCE has an underlying database with built-in security, backed up by copying to secure storage each night.

- Firewalls limit external access to REEID GCE network. Only authorised users with Company logins have access to the network: Customers and staff.

- Data Centres are strictly controlled access areas.

- The login gives access to REEID GCE network. Staff passwords expire after a defined period and must be changed by the user. Both Customers and staff are advised to change their passwords immediately if they believe their details have been compromised.

- Although workstations automatically lock if left inactive for a specific period, users are advised to always lock their workstations when moving away from their desk (windows key and L on a PC).

- Data stored on a network drive is backed up twice a day.

46. A range of specialist databases exist which contain varying levels of personal and sensitive information. The following should be adopted as good practice:

- Each database should be held in a separate directory on the main Company network drive and be password restricted to an authorised individual or group.

- The database itself should be password protected by the system administrator.

- All other personal or sensitive data that may be held in local, small-scale documents, for example spreadsheets and word documents, must be password protected and restricted to essential users.

- Personal or sensitive data should never be copied to a portable computer for local processing without the express permission of the system owner and only in exceptional circumstances. Whilst Company laptops are password protected, they can be vulnerable to a determined hacker. Equally, personal or sensitive data should not be stored on flash-drives, CD-ROM or other external devices.

47. Data at REEID GCE are retained and disposed of according to need. The overarching principle is that data should only be retained and stored for as long as such data have a legitimate purpose, and thereafter they should be disposed of securely. Each professional service area of the Company holds a Data Retention Schedule which specifies the nature of the data retained, the retention period, the reason for retention, and the action to be taken at the end of the retention period, including how the data are to be disposed of.

48. At the end of the retention period, data should be disposed of and/or destroyed. Manual files should be shredded and disposed of in designated confidential waste sacks if appropriate. Electronic

data should be deleted from central systems by the individual responsible for the data after liaising with the IT Services team.

Complaints

49. Individuals concerned about any aspect of the management of personal data at the Company may raise their concerns in the first instance with the owner of the corporate system involved (see Appendix 2) or the Company Secretary office. If the concern cannot be resolved, then a formal complaint may be made in accordance with the Complaints Procedure, using the form available on REEID GCE website. If an individual, having followed these procedures, is not satisfied that their complaint has been properly dealt with they may contact:

REEID GCE (UK) Limited

Management Office

uk@reeid.com

Responsibilities

50. Within this policy, the following post-holders have these responsibilities:

Responsibility	Owner
Administration of subject access requests, response to data protection enquiries from Customers.	Company Secretary
Initial investigation and management of data security breaches.	Company Secretary

Overall responsibility for Data Protection and Data Security Policy, authorisation of actions related to data security breaches, management and oversight of the Company Secretary, raising awareness of DPA across the Corporate, and the provision of training and information for staff	Management and Corporate Office
Overall responsibility for those aspects of data security relating to Company information technology systems	Head of IT Services
Strategic liaison regarding data protection and data security with the Executive Board	Company Secretary
Corporate approval of Data Protection and Data Security Policy	Executive Board
Personal data to be handled in line with the Company Data Protection and Data Security Policy, best practice and the Act	Staff and Customers handling personal data

Review

51. The policy will be reviewed in accordance with the corporate policy review schedule or when legislation is amended (whichever is the sooner) by the Executive Board in consultation with the Head of IT Services and Company Secretary.

References

52. The policy is supported within the context of the following pieces of legislation and Company policies:

- Data Protection Act 1998
- Data Protection and Freedom of Information Fees Regulations 2004
- Freedom of Information Act 2000
- Environmental Information Regulations 2004

- Privacy and Electronic Communications Regulations 2003
- Company Code of Practice for Managing Freedom of Information Requests
- Company ICT Acceptable Use Policy
- Company Data Retention Schedules (departmental)

Appendices

59. The policy is supported by the following documents:

- Appendix 1: Secure use of mobile devices;
- Appendix 2: Staff data protection notice;
- Appendix 3: Data Subject Access Request (SAR) Form (Staff);
- Appendix 4: Customer data protection notice;
- Appendix 5: Data Subject Access Request (SAR) Form (Customer);
- Appendix 6: Staff data collection consent - extract from Company, Contract of Employment (staff);
- Appendix 7: Data protection staff briefing

Appendix 1: Secure use of mobile devices

1. Purpose

The secure use of mobile devices addresses the Seventh Principle - Data Security and the Data Protection Act sets out the principles, expectations and requirements relating to the use of mobile devices and other computing devices which are not permanently located on Company premises.

This document should be read in conjunction with the Data Protection and Data Security Policy.

2. Definition

A mobile device is defined as a portable computing or telecommunications device which can be used to provide some of the functions typically associated with a desktop PC, such as storing or processing information. Examples include laptops, netbooks, tablets, smartphones, removable storage media (USB sticks/external hard drives) and wearable devices (Apple Watch/Pebble). As technology moves forwards this list is likely to expand.

3. Scope

All staff at the Company including contractors, service providers and other organisations that use mobile devices to access Company networks or information must comply with Corporate policy. It covers all mobile computing devices whether personally owned, supplied by the Company or provided by a third party. Non mobile devices that are not located on Company premises and are used for accessing Company networks or information are also in scope.

4. Personally owned devices

Whilst the Company does not require its staff to use their own personal mobile devices for work purposes, it is recognised that there is demand for this and it is often beneficial. The use of these devices is permitted subject to the following requirements and guidelines. Users must at all times give due consideration to the risks of using personal devices to access Company data and information:

Requirements

- An appropriate password/passcode must be set for all accounts on that device.
- A password protected screen saver or screen lock must be used.
- All devices must be set to lock automatically after a set period (5 minutes maximum) and require a password to unlock after this time.
- The device must run the latest version of the operating system and be updated with software updates/security patches in a timely fashion.
- All mobile devices used to access or store sensitive/confidential information must have the ability to be located and be remotely wiped, particularly smartphones and tablets.
- In the case of storage media all sensitive/confidential data stored on the device must be encrypted.
- Any devices at risk of malware infection must run anti-virus software.
- Any device used for this purpose should only be used by an authorised person. If family or friends are to use the device then it must be managed in such a way that others do not have access to this information.

Guidelines

- Do not undermine the security of the device for example by Jail Breaking an iPhone.
- Minimise the amount of sensitive/confidential data stored on the device.

- If a device needs to be repaired, ensure that the company have an agreement in place which guarantees the security of any data on the device.
- Do not leave devices unattended where there is a risk of theft.
- Be aware of people around you when entering passwords or using the device.

5. Company owned devices

REEID GCE will occasionally supply mobile devices to staff as required for their work. Where possible these devices will be configured in the same way as those which are permanently located on Company premises. Occasionally it is not possible to configure the device for the user, and it will be the responsibility of the user to set the configuration.

Whether the device is configured by REEID GCE prior to release or not, the requirements and guidelines listed above should be followed and the following additional requirements apply to any Company owned device:

- Non-members of the Company must not make any use of the supplied device.
- No unauthorised changes must be made to the supplied device.
- All devices must be returned to REEID GCE when they are no longer required or are in need of repair.

6. Third party devices

No staff should use any mobile device or other device that is for public use to access Company networks or information.

7. Lost equipment

Should a staff member at any time lose equipment that they believe contains sensitive/confidential content or allows access to REEID GCE network, this must be reported immediately to IT Services who can advise on the best course of action.

Appendix 2: Staff data protection notice

REEID GCE has a notification under the Data Protection Act 1998 to hold personal data about all members of its staff for the purposes of recruitment, appointment, training, remuneration, promotion and other employment related matters, including health and safety. The information is held in a variety of formats, including centrally managed databases. The Company has in place systems and procedures to ensure that information remains consistent and accurate throughout the databases and to enable the provision of staff services, such as the establishment of e-mail accounts and library membership.

Disclosure of data

Data will be processed in accordance with the provisions of the Act and will only be disclosed within the Company to members of staff who need to know it in order to carry out their duties, or to others connected with the Company for Company related activities or events. Data will only be disclosed to a third party outside the Company in accordance with the Act. This may include future employers who require verification of your period of employment.

Use of IT facilities

REEID GCE reserves the right to exercise control over all activities relating to its IT facilities and networks, including monitoring of systems and electronic communications and access to external electronic resources. This monitoring may include access to personal data held and managed on the IT facilities and networks. The reasons for undertaking such monitoring include ensuring adherence to REEID GCE's Guidelines for Use of IT Facilities.

Data retention

If you decide to leave, a permanent record of your period of employment at REEID GCE will be retained.

Your rights as a Data Subject under the Act

You have several rights relating to the personal data which REEID GCE holds about you. The main ones are as follows:

- To be given a copy of any data held, whether on a computer or in a manual file.
- To ask the Company not to process any data held about you on the grounds that it might cause you substantial damage or distress.
- To ask the Company not to use your personal data for the purposes of direct marketing, should this ever be undertaken by REEID GCE.

The Company has a Subject Data Access Request Form which is available on REEID GCE website with instructions for completion.

Your responsibilities as a Data User under the Act

You have three main responsibilities as a Company employee with respect to the processing of personal data:

1. If you hold personal data in any form, whether on computer or in a manual file, as part of your job, this must be registered with your business unit in a form accessible by the Data Controller whose responsibility it is to ensure the corporate data protection procedures are accurate and up-to-date.

2. In dealing with personal data as part of your job, you must ensure that it is not shared with anyone other than individuals connected to Company who need to know it to perform their work function. This covers both intentional disclosure and any disclosure that might happen by accident, for example through someone having oversight of your PC screen on which data is displayed. It is particularly important that personal details about members of staff or customers are not given to

anyone outside the Company without prior consent of the individual concerned. If you are in any doubt, please do nothing until you have sought advice;

Help and advice

You may seek help and advice about the Data Protection Act, and how it affects you both as a Data Subject and as a Data User, from your line manager in the first instance or from the Company Secretary / Director of HR / Head of IT Services.

Appendix 3: Data Subject Access Request (SAR) Form for Staff

I _____, wish to have access to data which the has about me in

the following categories: (Please tick as appropriate.)

- Employment references
- Disciplinary grievance and capability records
- Health and medical matters
- Political, religious or trade union information
- Any statements of opinion about my abilities or performance
- Personal details including name, address, date of birth etc.
- Other information: please list below

Signed

Dated

Appendix 4: Customer data protection notice

REEID GCE has a notification under the Data Protection Act 1998 to hold relevant personal data about its customers, for example, data about your business sign-up, background, methods of payment, accounting records and projects records, while in relation with Company. This data is processed by various Company administrative units. It is processed in accordance with the provisions of the Act and is only disclosed within the Company to members of staff who need to know it in order to carry out their duties or to others connected with the Company for Company-related activities or events. Where you provide a mobile telephone number, the Company may use this number to contact you by text message with relevant, Company-related information.

Specific disclosure of data

If you are involved in an emergency situation on Company premisses or in connection with Company field operations which results in you being hospitalised, REEID GCE may provide your emergency contact details to the relevant authorities dealing with the emergency, e.g. police, fire brigade or ambulance.

Use of IT facilities

The Company reserves the right to exercise control over all activities relating to its IT facilities and networks, including monitoring of systems and electronic communications and access to external electronic resources. This monitoring may include access to personal data held and managed on the IT facilities and networks. The reasons for undertaking such monitoring include ensuring adherence to REEID GCE's Guidelines for Use of IT Facilities.

Your rights as a Data Subject under the Act

You have several rights relating to the personal data which Company holds about you. The main ones are as follows:

- To be given a copy of any data held, whether on a computer or in a manual file.
- To ask REEID GCE not to use your personal data for the purposes of direct marketing.
- You will have the opportunity to object to these contacts if you wish. Further details about the surveys and what happens to the information that is collected can be obtained from the REEID GCE Secretary Office.

REEID GCE has established procedures for dealing with subject access requests which should be made using the appropriate form available on REEID GCE website.

The Company has a Subject Data Access Request (SAR) Form available on REEID GCE website which should be completed and submitted in accordance with instructions.

The Company Secretary Office will be pleased to help with any queries you might have about any of your rights under the Act.

Your responsibilities as a Data User under the Act

It is unlikely that you will find yourself processing personal data as part of your business relation at the Company. However, if you do, perhaps as part of a project, you will become a Data User under the terms of the Act and you will need to take certain steps to ensure that the Company knows what you are doing and that your processing of data

Help and advice

You may seek help and advice about the Data Protection Act, and how it affects you both as a Data Subject and as a Data User, from the Corporate Secretary Office.

Appendix 5: Data Subject Access Request (SAR) Form for Customers

I,_____, wish to have access to the data which the Company

currently has about me in the following categories either as part of an automated system or part of a relevant filing system: (Please tick as appropriate.)

- Business marks or relation details
- Business references
- Personal details including name, address, date of birth etc.
- Stored projects details including files and content
- Other information: please list below

Signed

Dated

Appendix 6: Staff data collection consent

Extract from REEID GCE Contract of Employment for all staff:

DATA PROTECTION

Company employees are required to comply with the provisions of the Data Protection Act 1998 and with the Company's Data Protection and Data Security Policy. By accepting this employment, you consent to the Company processing personal data relating to you as necessary for the performance of your contract of employment and/or the conduct of the Company's business. Further, you explicitly consent to the Company processing any sensitive personal data relating to you, including but not limited to self-certificates, doctors' certificates, medical reports, details of trade union membership or details of criminal convictions as necessary for the performance of your contract of employment and/or the conduct of the Company's business.

Appendix 7: Data protection staff briefing

All new staff to be given guidance during induction and updates provided at team meetings. What does the Data Protection and Data Security Policy mean to you?

As a publicly accountable body, REEID GCE is bound by the Data Protection Act (DPA) and is responsible for the protection of this type of information, termed 'sensitive data'. This means any personal information that can be specifically linked to an individual. The DPA covers data on current and former Customers and staff, potential Customers and staff, and members of the public. We therefore have to take reasonable measures to ensure that sensitive data is not put at risk of loss or theft. If the Company is successfully challenged under the DPA, there is a very real possibility of a hefty fine as well as subsequent scrutiny from the legislators.

The DPA gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly. The Company's obligations are:

■ to notify the Information Commissioner that REEID GCE is processing information;

■ to process personal information in accordance with the eight principles of the Act which make sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant, and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the individual's rights
- Secure
- Not transferred to other countries without adequate protection.

■ to answer subject access requests received from individuals. These may be staff, Customers or any individual who has an association with REEID GCE. They have important rights, including the right to find out what personal information is held on computer and most paper records.

What should you do?

Remote access has been facilitated so as a user you can access REEID GCE intranet and your files from any location. Therefore, there should be few reasons to transfer sensitive information away from your desk or access it outside of REEID GCE secure IT network. We do not recommend removing paperwork and storing information electronically on portable devices including laptops, memory sticks and disks. These are all vulnerable to loss or theft if left in cars, on public transport or in the home. Laptop and data loss from public sector organisations is commonly reported in the press and it would be regrettable if the Company made the headlines for a data security breach. Additionally, the Company is not insured for such losses and you may be open to REEID GCE Disciplinary Procedure. If you sometimes work from home or elsewhere offsite, you should only access sensitive data through the secure IT network.

Some of you will be presenting at conferences or meetings and will often take your presentation on a memory stick. This is normally not a risk as such data will be in the public domain when you present it so by definition is not sensitive. However, if you are dealing with sensitive information you must ensure you comply with the rules given below.

Rules

- Do not remove sets of sensitive information about staff, customers or the public from your work location or from the secure IT network; e.g. names and addresses of customers, projects details, job application forms etc.
- Keep your user ID and password for the IT network secret and secure.
- When working offsite, always access your documents by logging on to REEID GCE network and accessing your profile.
- Do not leave your laptop unlocked and unattended whilst logged on.
- Do not leave printed copies of sensitive data in plain view.
- Do not leave sensitive data on screen where others can see it.
- Do not disclose sensitive data to third parties without authorisation. If you are not sure how to handle a data request, contact REEID GCE Data Controller
- Do not copy sensitive data onto laptops, iPad or other mobile devices, e.g. flash drives, CD-ROMs, memory sticks. Even if your laptop/iPad is password protected, this is no barrier to a determined hacker.
- Always store data in your profile in Documents module, so that it is backed up every day. If you store information on the local drive it is not backed up and is vulnerable to theft.

- Never share your Company password with colleagues because you may have different levels of access to restricted areas within the network related to your roles within the organisation.
- Anonymise data if using it with an audience who are not authorised for full disclosure. However, be aware that with small subject groups it is sometimes possible to identify individuals even if names are not used. This should not be allowed to happen.