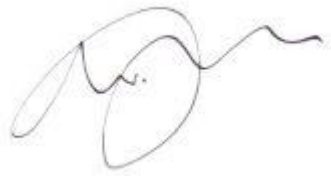
General Data Protection Regulation (GDPR) Policy

`

Version Control:

Date created	Created by	Next Review date
August 2017	Liz Moran	August 2022

Version Number & Date of amendment	Summary of amendments	Quality Board Member Approval Name	Signature	Date approved
3	General review	Mike Monaghan		12/01/21
4	Change of DPO	Mike Monaghan		19/08/21

Introduction

On the 25 May 2018 the General Data Protection Regulation (GDPR) will be applicable and the current Data Protection Act (DPA) will be updated by a new Act giving effect to its provisions. Before that time the DPA will continue to apply.

This Policy sets out the way personal data of staff, learners and other individuals is processed fairly and lawfully.

System Group collects and uses personal information about staff, learners and other individuals who come into contact with System Group. This information is gathered to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the System Group complies with its statutory obligations.

System Group is a data controller and processor and must therefore comply with the Data Protection Principles in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed. System Group must be able to demonstrate compliance. Failure to comply with the Principles exposes System Group and staff to civil and criminal claims and possible financial penalties.

Details of System Group's purpose for holding and processing data can be viewed on the data protection register: https://ico.org.uk/ESDWebPages/Entry/Z5761085

System Group's registration number is Z5761085. This registration is renewed annually and updated as and when necessary.

Aim

This Policy will ensure System Group;

- processes personal data fairly and lawfully and in compliance with the Data Protection Principles;
- all staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities under this policy;
- that the data protection rights of those involved with System Group are safeguarded;
- confidence in System Group's ability to process data fairly and securely.

Scope

This Policy applies to;

- personal data of all System Group the Board, employees, learners, parents and carers and any other person carrying out activities on behalf of System Group;
- the processing of personal data, both in manual form and on computer;
- all staff and Board members,
- use of CCTV

The Data Protection principles will ensure that personal data will be;

- processed fairly, lawfully and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed;

- accurate and, where necessary, kept uptodate;
- kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;
- processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

System Group can demonstrate compliance with these principles.

System Group has in place a process for dealing with the exercise of the following rights by the Board, staff, learners, parents and members of the public in respect of their personal data;

- to be informed about what data is held, why it is being processed and who it is shared with;
- to access their data;
- to rectification of the record;
- to restrict processing;
- to data portability;
- to object to processing;
- not to be subject to automated decision-making including profiling.

Roles and Responsibilities
The Board of System Group and the CEO are responsible for implementing good data protection practices and procedures within System Group and for compliance with the Data Protection Principles.

It is the responsibility of all staff to ensure that their working practices comply with the Data Protection Principles. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures forming part of this policy.

A designated member of staff, the Data Protection Officer, will have responsibility for all issues relating to the processing of personal data and will report directly to the CEO.

The Data Protection Officer will comply with responsibilities under the GDPR and will deal with subject access requests, requests for rectification and erasure, data security breaches complaints about data processing will be dealt with in accordance with System Groups Complaints Policy.
Data Security and Data Security Breach Management.

All staff are responsible for ensuring that personal data which they process is kept securely and is not disclosed to any unauthorised third parties. Access to personal data should only be given to those who need access for the purpose of their duties.

All staff will comply with System Groups Acceptable IT use Policy. Staff who work from home must have regard to the need to ensure compliance with this Policy and the Acceptable IT use Policy.

System Group uses closed circuit television (CCTV) and the images produced to prevent or detect crime and to monitor System Group buildings and grounds to provide a safe and secure environment for its Learners, staff and visitors, and to prevent loss or damage to property and surroundings. System Group's use of CCTV complies with the General Data Protection Regulation.

Data will be destroyed securely in accordance with the relevant legislation. New types of processing personal data including surveillance technology which are likely to result in a high risk to the rights and freedoms of the individual will not be implemented until a Privacy Impact Risk Assessment has been carried out.

System Group will have in place a data breach security management process and serious breaches where there is a high risk to the rights of the individual will be reported to the Information Commissioner's Office (ICO) in compliance with the GDPR.

All staff will be aware of and follow the data breach security management process.

All staff will be aware of and comply with the list of Do's and Don'ts in relation to data security in Appendix 1.

Subject Access Requests

Requests for access to personal data (Subject Access Requests) (SARs) should be sent to, and will be processed by, the Data Protection Officer. Records of all requests will be maintained.

System Group will comply with the statutory time limits for effecting disclosure in response to a Subject Access Request. The statutory time limit of 40 days continues until 25 May 2018 when under the GDPR the statutory time period reduces to one calendar month of receipt of the request.

The Company's Data Protection Officer is Mike Monaghan, Head of IT & Systems, and can be contacted on dpo@system-group.com.

Sharing data with third parties and data processing undertaken on behalf of System Group
Personal data will only be shared with appropriate authorities and third parties where it is fair and lawful to do so. Any sharing will be undertaken by trained personnel using secure methods.
Where a third party undertakes data processing on behalf of System Group e.g. by providing cloud based systems or shredding services, System Group will ensure that there is a written agreement requiring the data to be processed in accordance with the Data Protection Principles. Ensuring compliance

System Group suppliers and supply chain will be required to abide by System Groups Policy and sign an agreement to acknowledge their responsibilities having completed a GDPR compliance survey.

All new staff will be trained on the data protection requirements as part of their induction. Training and guidance will be available to all staff. All staff will read the Acceptable IT use

Policy.

System Group advises learners and Company employees whose personal data is held, the purposes for which it is processed and who it will be shared with. This is referred to as a "Privacy Notice" and is available on System Group website.

System Group will ensure Privacy Notices contains the following information;

- Contact Data Controller and Data Protection Manager;
- purpose of processing and legal basis;
- retentions period;
- who we share data with;
- right to request rectification
- erasure, to withdraw consent
- to complain, or to know about any automated decision making and the right to data portability where applicable.

Photographs, Additional Personal Data and Consents

Where System Group seeks consents for processing personal data such as photographs at events it will ensure that appropriate written consents are obtained. Those consent forms will provide details of how the consent can be withdrawn. Where the personal data involves a child under 16 years written consent will be required from the adult with parental responsibility.

Appendix 1

What staff should do:

- DO get the permission of your manager to take any confidential information home. This will only be granted as an exception.
- DO transport information from the office on secure computing devices (i.e. encrypted laptops and encrypted memory sticks). Wherever possible avoid taking paper documents out of the office.
- DO use secure portable computing devices such as encrypted laptops and encrypted USB memory sticks when working remotely or from home.
- DO ensure that any information on USB memory sticks is securely deleted off the device, or saved on a System Group shared drive.
- DO ensure that all paper based information that is taken of premises is kept confidential and secure, ideally in a sealed envelope which indicates a return address if misplaced.
- DO ensure that any confidential documents that are taken to your home are stored in a locked drawer.
- DO ensure that paper based information and laptops are kept safe and close to hand when taken off premises. Never leave them unattended. Particular care should be taken in public places (e.g. reading of documentation on public transport).
- DO ensure that when transporting paper documentation in your car that it is placed in the boot (locked) during transit.
- DO return the paper based information to System Group as soon as possible and file or dispose of it securely.
- Do report any loss of paper based information or portable computer devices to your line manager immediately.
- DO ensure that all postal and e-mail addresses are checked to ensure safe dispatch of information. When sending personal information by post the envelope should clearly state 'Private – Contents for Addressee only'.
- DO ensure that when posting/emailing information that only the specific content required by the recipient is sent.
- DO use pseudonyms and anonymise personal data where possible.

What staff must not do:

- DO NOT take confidential information to an entertainment or public place such as a pub or cinema, whether held on paper or an electronic device. Any information must be taken to the destination directly and never left unattended during the journey.
- DO NOT unnecessarily copy other parties into e-mail correspondence.
- DO NOT e-mail documents to your own personal computer.
- DO NOT store work related documents on your home computer.
- DO NOT leave personal information unclaimed on any printer or fax machine.
- DO NOT leave personal information on your desk overnight, or if you are away from your desk in meetings.
- DO NOT leave documentation in vehicles overnight.
- DO NOT discuss issues at social events or in public places.
- DO NOT put confidential documents in non-confidential recycling bins.
- DO NOT print off reports with personal data (e.g. pupil data) unless absolutely necessary.

- DO NOT use unencrypted memory sticks or unencrypted laptops

Appendix 2 – Supply Chain

Agreement System Group Limited:

GDPR Readiness

As I am sure you will be aware, new data protection requirements were imposed on all companies in the UK (and the rest of the European Economic Area) by the General Data Protection Regulation ("GDPR") on 25 May 2018.

You are a responsible and trusted provider of services to our business, and we ask that you work with us to have the necessary data processing agreement signed as soon as possible in order that we both comply with GDPR.

I am therefore writing to you to request that you provide certain necessary information that is required and to execute a data processing agreement, so we are both GDPR compliant.

To this end I enclose:

A questionnaire to be answered in relation to required data processing information regarding to your status as an organisation that has access to our learner personal data; and

A data processing agreement to bring in new data protection clauses so that our contract complies with the GDPR requirements.

Please would you execute the enclosed data processing agreement to bring in the new data protection clauses and return it to us. Please do not date the front page as this will be done upon System Group counter-signature. We will return a completed copy for your records.

Please would you return the executed data processing agreement to mike.monaghan@system-group.com

1. Data Processing Agreement

This Data Processing Agreement ("Agreement") is made between:

2. SYSTEM GROUP LIMITED and incorporated and registered in England and Wales with company number 03195134 whose registered office is at 2 A C Court, High Street, Thames Ditton, Surrey, KT7 0SR

Insert company name and registered address

("Supplier") (together the "parties" and the "party" shall be construed accordingly).

3. RECITALS
    a. The Supplier is the provider of services to System Group pursuant to an existing services agreement.
    b. System Group acts as the data controller of personal data processed in the course of carrying out the services. System Group also acts as the data controller of the personal data of its employees.
    c. The Supplier may from time to time process such data on behalf of System Group to enable the Supplier to provide services to System Group in accordance with the existing services agreement and System Group may make such data available to the Supplier in connection with this purpose.
    d. The Parties intend that the processing activities carried out by the Data Processor on behalf of the Data Controller shall comply with the provisions of this Agreement.

4. DEFINITIONS
    a. "Applicable Laws" means (i) any and all laws, statues, regulations, by-laws, orders, ordinances and court decrees that apply to the performance and supply of the Services, and (ii) the terms and conditions of any applicable approvals, consents, exemptions, filings, licences, authorities, permits, registrations or waivers issued or granted by, or any binding requirement, instruction, direction or order of, any applicable government department, authority or agency having jurisdiction in respect of that matter.
    b. "System Group Personal Data" means Personal Data provided or made available to the Supplier or collected or created for System Group in connection with this Agreement.
    c. Data Protection Legislation" means all Applicable Laws and codes of practice applicable to the Processing of Personal Data including (from 25 May 2018 only) the GDPR. "GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal 2 data and on the free movement of such data as applicable as of 25 May 2018, as may be amended from time to time.
    d. Model Clauses" means the standard contractual clauses annex to the EU Commission Decision 2010/87/EU of 5 February 2010 for the transfer of personal data to processors established in Third Countries (and any successor clauses), or any other standard contractual clauses issued by the EU Commission which replace such clauses from time to time.
    e. "Personal Data" means any information relating to an identified or an identifiable natural person (data subject) being one who can be identified, directly or indirectly, in particular by reference to an identification number or

to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity, or as otherwise defined under applicable Data Protection Legislation. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information shall be considered to be personal data.

f. "Process" or "Processing" or "Processed" means accessing, collecting, obtaining, recording, holding, disclosing, using, altering or deleting Personal Data, or carrying out any operation(s) on the Personal Data or as otherwise defined under applicable Data Protection Legislation.
g. "Security Incident" means the unauthorised acquisition, access, use or disclosure of System Group Personal Data.

5. EFFECTIVE DATE
    a. This Agreement shall take effect from and including 25 May 2018.

6. PROCESSING - *[Art 28, GDPR]*
    a. The Supplier is a data processor (or sub-processor) acting on System Group' behalf and shall use System Group Data in accordance with the provisions of this Agreement and System Group' documented instructions and only where necessary to provide the Services to System Group.
    b. The subject matter and duration of the Processing of the System Group Data is set out in this Agreement and the context and purpose for the Processing of System Group Data is to provide the services to System Group in accordance with the existing services agreement.
    c. The System Group Data that the Supplier may process is System Group' Employees' names, addresses, telephone numbers and associated information required for the services provided to System Group in accordance with the existing services agreement and in accordance with ESFA Rules. The Data Subjects are System Group' customers.
    d. The Supplier shall comply with and Process all System Group Personal Data in accordance with applicable Data Protection Legislation.
    e. The Supplier shall co-operate and assist System Group with any privacy impact assessments and consultations with (or notifications to) relevant regulators that System Group considers are relevant pursuant to Data Protection Legislation in relation to the System Group Personal Data and the Services. The Supplier shall procure that its personnel are obligated to maintain the security and confidentiality of any System Group Personal Data as provided in this Agreement and this obligation continues even after their engagement ends.
    f. The Supplier shall promptly forward to System Group and otherwise co-operate with and assist System Group at no charge with any requests from data subjects of any System Group Personal Data pursuant to Data Protection Legislation.
    g. The Supplier shall at System Group's option, delete (unless required by Applicable Laws) or return all copies of System Group Personal Data and cease Processing such System Group Personal Data after the business purposes for which the System Group Personal Data was Processed have been fulfilled, or earlier upon System Group's written request.
    h. The Supplier shall maintain a record of all categories of Processing

activities carried out on behalf of System Group which shall be made available to System Group upon request.

7. DISCLOSURE
    a. The Supplier will not disclose System Group Personal Data outside of the Supplier except:
        i. as System Group directs (including as permitted under this Agreement); or
        (ii) as required by Applicable Laws.
        ii. in the event that the Supplier receives any request for disclosure of System Group Personal Data by a law enforcement person or agency the Supplier will, to the extent allowed by Applicable Laws, including the terms of the third party request itself, attempt to redirect the law enforcement agency to request that data or information directly from System Group.
        iii. promptly notify System Group of receipt of the request and use commercially reasonable efforts to comply with System Group' reasonable requests regarding its efforts to oppose the request.
        iv. If compelled to disclose System Group Personal Data to law enforcement, then the Supplier will promptly notify System Group and provide a copy of the demand, unless prohibited by Applicable Laws from doing so.
        v. In the event that the Supplier receives any request for disclosure of (or information in relation to) System Group Personal Data in a circumstance not covered by the above:
        vi. Supplier shall promptly forward such request to System Group; and
        vii. at no charge, co-operate and assist System Group with such request where so directed by System Group (including in relation to requests from data subjects pursuant to Data Protection Legislation).

    b. The Supplier shall procure that its personnel are obligated to maintain the security and confidentiality of any System Group Personal Data as provided in this Agreement and this obligation continues even after their engagement ends.
    c. The Supplier shall promptly forward to System Group and otherwise co-operate with and assist System Group at no charge with any requests from data subjects of any System Group Personal Data pursuant to Data Protection Legislation.
    d. The Supplier shall at System Group's option, delete (unless required by Applicable Laws) or return all copies of System Group Personal Data and cease Processing such System Group Personal Data after the business purposes for which the System Group Personal Data was Processed have been fulfilled, or earlier upon System Group's written request.
    e. The Supplier shall maintain a record of all categories of Processing activities carried out on behalf of System Group which shall be made available to System Group upon request.

8. SECURITY - [Arts 28 and 32 GDPR]
    a. The Supplier has implemented and will maintain throughout the term of this Agreement appropriate technical and organizational measures, internal

controls and information security routines intended to protect System Group Personal Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction. These shall at all times:

i. be of at least the minimum standard required by Data Protection Legislation; and
ii. be of a standard no less than the standards compliant with good industry practice for the protection of Personal Data; and
iii. compliant with any minimum standards and/or requirements that System Group may provide the Supplier from time to time in writing, to ensure a level of security for the System Group Personal Data appropriate to the risk and to assist System Group and its Affiliates in ensuring compliance with the requirements for the security of Processing as set out in Data Protection Legislation.

b. The Supplier shall ensure that all System Group Personal Data is encrypted at all times both in transit and at rest whilst in the possession or under the control of the Supplier. The level of encryption applied should be determined based on good industry practice and the state of technology available at the time.

9. NOTIFICATION AND INCIDENTS - *[Arts 33 and 34]*

a. If the Supplier becomes aware of or reasonably suspects that any Security Incident has occurred, the Supplier will without undue delay (and in any event within twenty-four (24) hours):
   i. notify System Group of the Security Incident;
   ii. investigate the Security Incident and provide System Group with detailed information about the Security Incident including making available a suitably senior, appropriately qualified individual to discuss any concerns or questions System Group may have;
   iii. take reasonable steps to mitigate the effects and to minimise any damage resulting from the Security Incident and assist System Group in remediating or mitigating any potential damage from a Security Incident to the extent that such remediation or mitigation is within the Supplier's control as well as reasonable steps to prevent a recurrence of such Security Incident.

10. SUBCONTRACTORS - *[ART 28, GDPR]*

a. System Group acknowledges and consents to the Supplier permitting sub-contractors to Process System Group Personal Data strictly subject to the terms of this Agreement and providing that the Supplier shall notify System Group of any intended change concerning the addition or replacement of any sub processor within a reasonable period before such addition or replacement.
b. Following receipt of such information System Group shall notify the Supplier if it objects to the new sub processor. If System Group does not object to such sub processor within thirty (30) days of receiving the information, System Group shall be deemed to have accepted the sub processor. If System Group has raised a reasonable objection to the new sub processor and the parties have failed to agree on a solution within

fourteen (14) days of the date of receipt of such objection, then System Group may terminate this Agreement and any contract relating to the Processing upon seven (7) days' written notice.

c. The Supplier is fully liable to System Group for any acts or omissions of the subcontractor in regard of its Processing of Personal Data.

d. The Supplier shall ensure that subcontractors shall be contractually bound to the same obligations with respect to the Processing of System Group Personal Data as to which the Supplier is bound by this Agreement relating to security and audit and otherwise.

11. TRANSFER OF DATA

a. Save as set out herein, or as System Group may otherwise authorise, the Supplier will not transfer to any third-party System Group Personal Data.

b. The Supplier (or any subcontractor) shall only transfer System Group Personal Data from the UK or EU to a country outside the European Economic Area ("EEA") where System Group has provided its written approval to such transfer. Approved transfers as at the effective date of this Agreement are set out in Annex 1.

c. Transfers shall only be permissible:

i. where the entity receiving the System Group Personal Data is located in a territory which is subject to a current finding by the European Commission under applicable Data Protection Legislation that it provides adequate protection for Personal Data;

ii. the Supplier and the entity receiving the System Group Personal Data has entered into the Model Clauses or is subject to an alternative mechanism approved by relevant authorities pursuant to Data Protection Legislation to the extent that such Model Clauses or other mechanism continue to be recognised and accepted by the relevant authorities as a legitimate basis for transfer of Personal Data; or

iii. the necessary statutory approvals required to be obtained by the Supplier (or subcontractor) as a data processor (or sub-processor), if any, have all been obtained to enable the transfer of the System Group Personal Data.

iv. Where System Group (as opposed to the Supplier or subcontractor) is the exporting entity, the Supplier shall procure that the entity receiving the System Group Personal Data pursuant to this paragraph, enters into Model Clauses with System Group (or such other mechanism as System Group shall elect) prior to any such transfer taking place. Where the Supplier is itself the importing entity receiving the System Group Personal Data, it shall itself enter into the Model Clauses with System Group (or such other mechanism) under this paragraph.

v. To the extent that any Processing of System Group Personal Data by the Supplier (or subcontractor) pursuant to this Agreement may involve the transfer of such System Group Personal Data out of the country in which it is held and such transfer is not covered by this agreement and

vi. the Supplier (or any subcontractor) shall only transfer that System Group Personal Data where System Group has provided its written

consent to such transfer. Such transfers shall only be permissible where any measures required under Data Protection Legislation are in place and remain valid.

12. AUDIT - *[Art 28(3)(H), GDPR]*
    a. Subject to reasonable written advance notice, the Supplier shall permit System Group and/or a qualified representative (subject to reasonable and appropriate confidentiality undertakings) to conduct during normal working hours periodic security scans and audits of the Supplier's (or its subcontractors') systems and processes in relation to the Processing of System Group Personal Data and shall comply with all reasonable requests or directions by System Group to verify and/or procure that the Supplier is in full compliance with its obligations under this agreement. The Supplier shall promptly resolve, at its own expense, all security issues discovered by System Group and reported to the Supplier.
    b. System Group shall have the right following any such audit to request additional safeguards, establish back-up security for System Group Personal Data and keep back-up System Group Personal Data and System Group Personal Data files in the Supplier's (or its subcontractors) possession. The parties shall agree on the additional safeguards to be implemented, if any.

13. WARRANTY AND INDEMNITY
    a. The Supplier represents and warrants that:
        i. it complies with all applicable Data Protection Legislation; and
        ii. the Processing of System Group Personal Data described in or contemplated by this Agreement and that the Processing of System Group Personal Data by the Supplier in accordance with the written instructions from time to time of System Group shall not cause System Group to be in breach of the Data Protection Legislation. Without prejudice to any other right or remedy which System Group may have the Supplier shall indemnify System Group in full and on demand against all liabilities, costs, expenses, penalties, damages and losses of whatever nature (including any legal and other professional costs and expenses) suffered or incurred by System Group arising out of or in connection with any breach by the Supplier of this Agreement.

14. VARIATIONS
    a. No variation of this Agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

15. ASSIGNMENT AND OTHER DEALINGS
    a. The Supplier shall not assign, novate, subcontract, transfer, mortgage, charge, declare a trust over or deal in any other manner with any of its rights and obligations under this Agreement.

16. GOVERNING LAW AND JURISDICTION
    a. This Agreement and any dispute or claim arising out of or in connection with

it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of England and Wales.

b. Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims).

Name:	
Title:	
Signed for and on behalf of System Group	

Name:	
Title:	
Signed for and on behalf of Enter company name	

System Group GDPR Questionnaire

System Group Limited is the data controller for the Personal Data of its Learners and participating employers.

System Group contracts with various suppliers for the provision of various ancillary services, and these suppliers are data processors for the System Group' Personal Data. GDPR requires System Group to undertake due diligence with its suppliers to ensure that System Group Personal Data is processed in accordance with the GDPR.

Name of Organisation	
Contact Name	
Locations Covered	
Completed By	
Completed Date	

For the purposes of this questionnaire -

"System Group Personal Data" means Personal Data provided or made available to you or collected or created for System Group in connection with your provision of the services to System Group by you.

"Personal Data" means any information relating to an identified or an identifiable natural person (data subject) being one who can be identified, directly or indirectly or as otherwise defined under applicable Data Protection Legislation.

1. DATA COLLECTION

What System Group Personal Data is processed? (eg name, address, telephone number, etc.)

2. DATA STORAGE AND ARCHIVING

2.1 How do you store System Group Personal Data? (eg on computer and/or manual files and/or personal devices)

- Please give details of the relevant databases or filing systems.
- Please include details of how personal data is treated in emails and what encryption techniques are employed.

2.2 Are all manual files and/or computer data stores internal to your organisation, or is third-party data storage used?

- Please detail any third-party companies, their location, and how data is stored.

2.3 In what format, or in what medium, is System Group Personal Data backed up or archived? Where is the backup or archive data stored?

Please note: If data is held by a third party that third party is acting as a sub-processor. The Sub-Processor section of this form must be completed to assess the relationship.

3. SECURITY

3.1 Describe in detail your security procedures in operation to keep System Group Personal Data secure. Describe the physical, administrative, and technological procedures in force.

3.2 What firewall protection and anti-virus protection is in place?

3.3 Who has access to System Group Personal Data within your organisation? Who has access to such data from outside the organisation?

3.4 What policies and procedures are in place to detect and deal with data breaches and to report them to System Group?

4. DESTRUCTION OF DATA AND TERMINATION OF CONTRACT

If the System Group requires, how will you destroy System Group Personal Data?

5. SUB-PROCESSORS

5.1 Are any of your data processing activities for System Group Personal Data carried out by third parties (sub-processors)? Please list and describe all such activities.

5.2 What written agreements are in place governing these sub-processing arrangements?

5.3 Outline the security measures required of each sub-processor.

5.4 Do the sub-processors use any other organisation to perform that service on their behalf? If so, list the organisations and any written arrangements in place for these sub-contractor services.

6. TRANSFERS OF SYSTEM GROUP PERSONAL DATA

6.1 Is there any transfer of System Group Personal Data to third parties outside your organisation?

6.2 If so, how is such data transferred? (e.g. encrypted email, secure ftp)

6.3 In what countries are the people to whom such data is disclosed, whether inside or outside of your business, located?

6.4 Where such data is transferred outside the EEA, what measures are in force to ensure compliance with the Eighth Data Protection Principle? (e.g. EU Model Clauses, binding corporate rules)