National Records of Scotland

Data Protection Code of Practice
Business Information

July 2016

CONTENTS

1. Introduction

1.1 National Records of Scotland (NRS) is required by law to comply with the Data Protection Act 1998 (DPA) which was enacted to ensure the fair and lawful processing of personal data. This code of practice has been drawn up to ensure NRS complies with the legislation by following organisation wide policies and procedures for the management and administration of information created or received by us in the course of our business transactions. This code applies solely to NRS business documentation. It does not apply to the archival collections transferred to NRS for permanent preservation, which are the subject of a separate code of practice.[1] It also does not apply to statistical data which is subject to the Code of Practice for Official Statistics[2] and several other official guidance documents.[3]

1.2 NRS regards the lawful and correct treatment of personal information as integral to successful business operations and to maintaining the confidence of our customers and stakeholders. Our commitment to effective data protection is supported by the NRS Data Protection Policy. This requires every member of staff to familiarise themselves with and follow NRS data protection policy, guidance and practices, of which this code forms a part.

2. Collection and Processing of Personal Data

2.1 In the course of our business transactions NRS will collect and process various sets of personal and sensitive personal data[4]. The DPA is designed to ensure that this data is kept accurate, up-to-date and is processed fairly and lawfully.

2.2 When collecting personal data, whether from clients, customers or colleagues, you should always carefully consider why the information is being collected and what you are going to do with it. At all times your approach should be to question the relevance of the data being collected. All personal data requested for processing must be relevant to the processing it supports. Excessive or irrelevant data cannot be collected. It is also important to remember that the storage of information has a cost and brings legal liability with it so you should always ask yourself whether you really need the information you are asking for. [5]

2.3 When collecting personal and sensitive personal data, staff should always take time to explain to the data subject their rights under the DPA. Data subjects have the

[1] Please see the *Data Protection Code of Practice: Archive Collections.*
[2] Please see https://www.statisticsauthority.gov.uk/monitoring-and-assessment/code-of-practice/ for further information.
[3] Including the National Statistician's Guidance (see http://www.statisticsauthority.gov.uk/national-statistician/ns-reports--reviews-and-guidance/national-statistician-s-guidance/index.html); Statistician Group guidance on (i)Data Management (see http://intranet/InExec/AboutUs/Professional-Groups/StatisticianGroup/StandGuidProced/Guidance/DataMgement/overview); and (ii) Legislation and Standards (see http://intranet/InExec/AboutUs/Professional-Groups/StatisticianGroup/StandGuidProced/StandardsProcedures/Overview)
[4] For further information and a definition of personal and sensitive personal data, please refer to the NRS Data Protection Policy.
[5] Privacy Impact Assessments can help with this, please see Section 4 for further details.

right to be informed of the identity of the data controller and the intended purposes of processing. Anyone collecting personal data should be open about why they are doing so and how they intend to use the data. Please refer to Section 3: Privacy Notices, for further information.

2.4 Any collection and processing of personal data must be justified by one of the conditions set out in Schedule 2 of the DPA. The conditions that may be applicable in NRS are:

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at the data subject's request to enter into a contract;
- The processing is necessary to ensure compliance with any legal obligation other than that imposed by a contract;
- The processing is necessary to protect the vital interests of the data subject;
- The processing is necessary for the administration of justice, for the exercise of any functions conferred by any Act, for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or for the exercise of any other functions of a public nature in the public interest;
- The processing is necessary for the legitimate interests of the data controller or third party recipients providing it is not prejudicial to the rights and legitimate interests of the data subject.

And any collection and processing of sensitive personal data must be further justified by one of the conditions set out in Schedule 3 of the DPA. The conditions that may be applicable in NRS are:

- The data subject has given their explicit consent to the processing;
- The processing is necessary to meet legal rights or obligations in connection with employment;
- The processing is necessary to protect the vital interests of the data subject or another person where consent cannot be obtained;
- The information in the personal data has been made public as a result of the deliberate actions of the data subject;
- The processing is necessary for legal proceedings, obtaining legal advice, or otherwise establishing, exercising or defending legal rights;
- The processing is necessary for the administration of justice, for the exercise of any functions conferred by any Act, for the exercise of any functions of the Crown, a Minister of the Crown or a government department;
- The processing is necessary for medical purposes carried out by a health professional or a person who owes an equivalent duty of confidentiality;
- The processing is of personal data relating to racial and ethnic origin and is necessary to monitor and promote equality of opportunity;
- The processing is in circumstances specified by an order of the Secretary of State.

These conditions do not need to be met when processing "category (e)" personal data[6], that is, in layman's terms, data which are not recorded for processing

[6] Please see https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/ for further information.

by computer or for keeping in a filing system, and which are not certain types of health, educational, housing or social services record (see the reference).

3. Privacy Notices

3.1 When collecting personal data, we must provide an explanation to the individual as to why we need their data, what we will use it for, who we will share it with (and what they will use the data for), how the individual can access the information held about them, and how we will ensure that the data is kept securely. We should also consider whether or not we are likely to want to use the data for a different purpose in future. This information should be provided in a short and simple statement, written in plain English, in the form of a Privacy Notice.

3.2 Further to this information, it is recommended that you tell individuals:

- how long we will keep the data;
- whether or not elements of the collection process are optional or mandatory;
- what the consequences may be of not collecting the data;
- if the information is to be transferred overseas;
- who they can contact if they want to find out more information or make a complaint; and
- how they can make a complaint to the Information Commissioner, if they wish to do so.

3.3 It is important to note that in some cases, individuals will not have a choice about whether or not their personal data is collected – for example, in order to provide a service or carry out a transaction requested by them – therefore it would be inappropriate to ask for their consent as it is meaningless. In order to ensure transparency and ensure that the collection of data is fair, NRS should inform users why the data is being collected and what it will be used for (but see paragraph 3.6).

3.4 If an individual has a choice over whether or not the data is collected or what it will be used for, we must inform them of this choice and respect their decision.

3.5 If you think an individual would be surprised about your use of their data, or would find it objectionable in any way then it is necessary to tell them about it. This is ‘actively communicating’ a privacy notice and means that we will actively inform an individual of the collection and processing of their personal data. This is different to having a privacy notice available for individuals to access if they want to find out more about how we handle personal information. It is also necessary to actively communicate a privacy notice when:

- collecting sensitive personal data;
- the provision of their personal data, or a failure to do so, would have a significant effect on the individual;
- the information will be shared with another organisation in a way that wouldn’t be expected;

- you hold information now that you want to use in a different way to the purpose for which it was originally collected; or
- you now wish to share it with an organisation when you have explicitly stated that you would not do so.

3.6 Privacy notices do not need to be actively communicated if the collection and use of the data:

- is something that a reasonable person is likely to anticipate and would agree to if asked;
- is necessary to carry out the transaction or deliver the service the individual has requested; and
- will have no unforeseen consequences for the individual concerned.

However, in these cases it is still necessary to have a privacy notice available for an individual to access if they want to find out more information about how the data will be managed by NRS.

3.7 It is recommended therefore, when collecting personal data for use by NRS, you provide the person contributing the data with the following information:

a) The identity and address of the data controller: The Registrar General / Keeper of the Records of Scotland, National Records of Scotland, HM General Register House, 2 Princes Street, Edinburgh, EH1 3YY.
b) A brief description of the purposes for which the data will be used.
c) Details of any third parties to whom the data will be disclosed and the opportunity for the data subject to indicate if they consent or dissent.
d) Notice if it is intended to transfer the data outside the European Economic Area (EEA) and the opportunity for the data subject to indicate if they consent or dissent.
e) Details of how to seek access to the data and correct any inaccuracies in it.

This information should be written clearly and prominently placed on the data collection form. A sample copy of the data collection form should be retained for as long as the data itself is retained.

3.9 When making privacy notices available, please ensure that you use the same medium to deliver the notice as you are using to collect the information. For example, if you are collecting the information via a website, then the privacy notice should be available on the website also.

3.10 Colleagues should also ensure that all privacy notices in place within NRS are regularly reviewed in order to ensure they remain relevant, accurate and up-to-date. It is also important to measure the effectiveness of all privacy notices by reviewing any complaints received about the collection and processing of personal data within NRS or the privacy notices themselves.[7]

[7] Please notify the Data Protection Officer of any complaints received about the handling of personal data or the use of privacy notices.

4. Privacy Impact Assessments

4.1 NRS uses privacy impact assessments (PIAs) to help us identify the most effective way of complying with our data protection obligations and meeting individuals' expectations of privacy.

PIAs are a tool organisations can use to identify and reduce risks to privacy. They help minimise the risks of harm to individuals through the misuse of their personal information.

It is NRS policy to carry out PIAs for all projects which involve the handling of personal data and which may have an impact on privacy. The meaning of project here is broad and as well as formal programmes and projects, takes in any new plan, proposal, initiative, system or process.

Our use of PIAs helps ensure NRS follows an approach of privacy by design. We use PIAs to systematically analyse how a particular project will affect the privacy of individuals and address and resolve any issues which are identified at an early stage. This methodology enables the design of more efficient and effective processes for the handling of personal data.

The Information Commissioner has issued a code of practice on conducting privacy impact assessments and NRS complies with this code.[8]

4.2 The benefits of PIAs and Privacy by Design are:

- Understanding privacy risks and taking a privacy by design approach helps us minimise risks and build trust.
- Designing projects, processes and systems with privacy in mind from the outset helps us identify potential problems at an early stage.
- Early resolution of problems is usually simpler and more cost effective.
- Heightened awareness of privacy and data protection across NRS.
- Ensuring NRS meet all legal obligations and is compliant with the DPA.
- Ensuring individuals' rights to privacy are protected.

4.3 The PIA Process

A PIA will be coordinated by a key member of the project team who has the authority to influence processes and decision making. The PIA process is documented in a report. NRS uses a template for the report to ensure consistency of approach. The PIA process follows these steps:

Step 1. Identifying the need for a PIA
The potential requirement to conduct a PIA is included within NRS programme project management process and guidance. We use the screening questions in the ICO code of practice to help identify whether a PIA is necessary. If it is clear that a project involves personal data or will have some impact on privacy then a PIA will be

[8] ICO Conducting privacy impact assessments code of practice: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

carried out. If a PIA is not required then a record of how that decision was reached will be retained.

Step 2. Consulting with stakeholders
We will **c**onsult with relevant internal and external stakeholders throughout the PIA process to allow people to highlight privacy risks and solutions based on their own area of interest or expertise.

Step 3. Describing information flows
In the PIA report we will explain how information will be collected, used, and retained.

Step 4. Identifying the privacy risks
In the PIA report we will identify and record any privacy risks which become apparent. We will carry out a compliance check against the DPA and any other relevant legislation. We will assess corporate risks, including the risk of regulatory action, reputational damage, or the loss of public trust.

Step 5. Identifying risk mitigation actions and privacy solutions
If any privacy risks are identified we will decide on appropriate actions to eliminate, reduce or accept these risks, in agreement with project stakeholders. We will devise solutions which mitigate risks and integrate these into the project. Any privacy risks which have been accepted as necessary for the project to continue will be recorded.

Step 7. Review by NRS Privacy Impact Group
The NRS Privacy Group will review the PIA and evaluate the privacy impacts and public benefits of the proposed activity. The group is made up of information specialists across NRS. It provides an independent perspective on whether the benefits are proportionate to the risk to privacy given the risk management in place.

Step 8. Signing off PIA outcomes
Solutions or mitigations for each risk are recorded as outcomes in the PIA report. The PIA report is authorised and signed off by the Information Asset Owner (IAO).

Step 9. Integrating PIA outcomes back into project plan
The agreed outcomes and actions will be integrated into the project plan. As with all risk management activities the PIA is an ongoing process and will continue to be updated throughout the life of the project.

4.4 For further information about PIAs, including advice on when it might be appropriate to conduct a PIA, please contact the Data Protection Officer.

5. Disclosure to Third Parties

5.1 There are a number of well-established circumstances in which NRS legitimately provides personal data to third parties, such as the sale of extracts from the register of births and the supply of individual records of births to NHS boards and researchers. However, there are very few other instances where we would disclose personal data to third parties without the data subject's prior consent. Consent

should usually always be sought first by referring requests for personal data to the data subject directly. One exception would be to respond to an urgent request from a confirmed, reliable source, when the data subject's consent cannot be obtained and disclosure is necessary to protect the 'vital interests' of the data subject. The Information Commissioner considers 'vital interests' to be matters of life and death.

5.2 Consent can be set aside only if any delay will endanger the health and welfare of the data subject, their dependants or that of another person where this is dependant on the disclosure. We should give consideration to the balance of benefit and harm arising from disclosure. A significant gain to a third party can outweigh a minor inconvenience to a data subject. A judgement should be formed as to the reasonableness of disclosing the data according to the circumstances. A medical emergency or some other time critical event could meet the criteria.

5.3 We must be sure that the third party is trustworthy and that there exists an urgent need for disclosure. Not all requests may be honest. Some can be invasive or a risk to personal safety and security. Official requestors will respect your caution. They should be similarly aware of the need to protect personal data and are likely to operate similar procedures in their own place of employment. We should keep a record of third party requests for personal data and of any disclosures made without consent and inform data subjects of these.

5.4 When obtaining or giving out personal data over the telephone staff should be careful to request or supply only relevant information. For example you should not take a caller's address unless you intend to visit or send something to that address. We can supply names, work numbers and responsibilities from the staff directory or put callers through to staff and work areas directly. We should not disclose work locations to protect staff going from and to their workplace. We should not disclose personal information such as home phone numbers, addresses or work locations to third parties. Instead we should request the caller's contact details to pass on, so that staff can respond personally.

6. Notification

6.1 Notification is the process by which a data controller informs the Information Commissioner's Office (ICO) of all processing operations that involve personal data. Failure to notify is a criminal offence.

6.2 Notification is renewed annually and any amendments should be made as required. When any part of our entry becomes inaccurate or incomplete we must inform the ICO as soon as practicable and in any event within 28 days. NRS's notification can be viewed on the public register available on the ICO website[9]. If you conduct a process which is not mentioned on the notification you must contact the Data Protection Officer immediately so that it can be updated.

6.3 The Data Protection Officer will maintain an inventory of personal data systems to inform the annual renewal of our notification to the ICO. A personal data audit will be

[9] Please see https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

carried out annually to ensure the inventory is up-to-date. Colleagues should complete a Personal Data Audit Form to notify the Data Protection Officer of any new processing being undertaken (see Annex A).

7. Subject Access Requests

7.1 The DPA affords data subjects certain rights including:

- right of access to inspect data held about them;
- right to prevent processing of data;
- right to sue for damage caused by wrongful processing.

The most fundamental of these is the right to access. Data subjects are entitled to know what personal data an organisation holds about them and to request a copy of this data in a form that is comprehensible. These requests are known as Subject Access Requests and must be processed within 40 days.

7.2 All subject access requests must be submitted in writing. Anyone making an oral request should be asked to complete a *Subject Access Request Form*.[10]

7.3 Subject access requests for access to personal information created and processed by NRS, will be handled in the first instance by the Data Protection Officer. However, it is important to note that NRS staff may be required to provide assistance in identifying the data. Subject access requests for access to personal data in open historical records should be referred to the search rooms and the enquirer will be provided with access to the records in accordance with the usual arrangements for readers or remote researchers.

7.4 NRS is legally required to respond to subject access requests within 40 calendar days, so there should be no delay in the processing of requests. Please ensure that all requests are forwarded to the Data Protection Officer at the earliest opportunity.

7.5 Where personal data are used for research, statistical or historical purposes, the personal data may be exempt from the data subject's right of access, provided that the research results, or any resulting statistics, are anonymised.

8. Managing Personal Data in Current Records and Emails

8.1 Personal data should never be stored on the local hard drives of office desktop computers or laptops, which are not secure. Staff should instead use the appropriate corporate or personal workspace on network drives to which access is controlled. Staff must not store any personal data on unencrypted USB pens or laptops.

8.2 Staff using laptops outside the office should not leave them unattended and should exercise due care to prevent any unauthorised personnel from accessing personal data on NRS systems.

[10] The form is available on our website and in our search rooms.

8.3 Emails, both incoming and outgoing, are covered by the DPA if one or other of the following criteria is met:

- The sender or recipient is identifiable, either through their email address or the content of the email, or;
- The text of the email contains personal data, i.e. facts, opinions or intentions about identifiable living individuals.

Staff should be aware that their emails may be monitored for legitimate purposes – for answering subject access requests and ensuring compliance with the DPA.[11]

8.5 Paper files, containing personal data, must be stored securely at all times with access restricted to personnel with the necessary authorisations to view the data. Semi-current paper files can be sent to the Records Management Unit for secure storage.[12]

9. Employee Personal Data

9.1 In NRS most of our official personnel functions are conducted by the Human Resources function in Scottish Government and they retain appropriate records. Attendance management returns and staff performance appraisal markings are now recorded on the eHR system. However, we do still conduct staff monitoring and development meetings and copies of these can be stored in your Home folder in eRDM or your H:\ drive.

9.2 Good practice for line managers:

- Ensure all staff are aware of all information which will be kept about them, how it will be used and to whom it will be made available;
- Ensure staff are made aware of their rights under the DPA, including the right of access to information kept about them;
- Relevant employee personal data should be retained by Scottish Government Human Resources or on a line manager's personal workspace.

10. NRS Websites

10.1 Privacy notices should be made available on all NRS websites[13] to inform stakeholders how we collect, use and store personal information gathered through the websites.

[11] Please see the *Managing Email Policy* for further information.
[12] Please contact the Data Protection Officer for further information about this service.
[13] At present, this includes the following websites: NRS, NAS, Scottish Documents, Scottish Handwriting, ScotlandsImages, ScotlandsPeople, Scottish Archive Network, Scottish Archives for Schools, The Scottish Register of Tartans, the National Register of Archives for Scotland, and Scotland's Census.

10.2 If cookies are used, we must provide clear and comprehensive information about the purposes of the storage of, or access to, that information and obtain consent from visitors to the website for their use.

10.3 If we collect personal data via online forms on our websites then the data subject should be provided with a privacy notice explaining the intended use of their personal data. On each occasion where personal data is exchanged via the website a link to the privacy notice should also appear to remind the data subject that they are passing on their personal data.

10.4 Any personal data gathered through a website must be transmitted and stored securely. Personal data must not be displayed on any web page.

11. Closed Circuit Television (CCTV)

11.1 NRS operate CCTV cameras in all of our buildings, both inside and outside of the buildings, in order to prevent crime, to detect, apprehend and prosecute offenders, and to protect staff and property. The Scottish Government Control Room are responsible for monitoring, recording and facilitating access to CCTV images from our Edinburgh buildings for NRS. Legal responsibility for the fair processing of CCTV in NRS buildings resides with The Registrar General / Keeper of the Records of Scotland and The Scottish Government. The operation of the CCTV system is regulated by:

- The Scottish Government CCTV Code of Practice, April 2010
- Closed Circuit Television (CCTV) and the Data Protection Act 1998: Guidance Notes for The Scottish Government Buildings, Associated Departments, Agencies and other Government Departments, 2006
- The Scottish Government CCTV Operational Procedure Manual, April 2010

11.2 The Estates Team are responsible for ensuring that people know that they are in an area where CCTV surveillance is being carried out. They meet this obligation through the use of clearly visible signage in and around the surveillance area.

11.3 All requests for access to recorded images and/or determining disclosure are the responsibility of the Data Protection Officer or the Accommodation Manager. All requests for access should be recorded on the ‘CCTV Access and Disclosure Form’ (see Annex B) and a copy sent to the Data Protection Officer to action and retain on file.

11.4 Disclosure of recorded images to third parties should only be made in limited and prescribed circumstances. Acceptable reasons for disclosure include:

- Law enforcement agencies where the images recorded would assist in a criminal enquiry;
- Prosecution agencies;
- Relevant legal representatives;

- The media, where it has been decided that the public's assistance is needed in order to assist in the identification of a victim, witness or perpetrator in relation to a criminal incident;
- People whose images have been recorded and retained.

11.5 Any enquiries relating to the use and operation of CCTV should be referred to the Data Protection Officer or the Accommodation Manager.

12. Use of Third Party Contractors

12.1 The Registrar General / Keeper of the Records of Scotland, as data controller for NRS, is responsible for the fair and lawful processing of all personal data subject to the provisions of the DPA. If we employ any third party, whether an individual or company, to perform any task or service on our behalf which involves the processing of personal data, we must ensure that they also adhere to the provisions of the DPA. This is best provided for in a written contract. It is essential we do this as it is the data controller, not the data processor who is directly obliged to comply with the DPA. Therefore any breach of compliance, even solely by the data processor, would remain the responsibility of NRS.

12.2 When we employ contractors to perform tasks for us we must assess whether these will involve any processing of personal data. Examples of data processing include:

- data inputting
- couriering
- internet service provision
- waste disposal
- cleaning which involves access to areas where data is held
- printing/publishing
- building work which involves access to areas where data is held
- disaster recovery

12.3 Any contractor who is selected to act as a data processor must offer sufficient assurances that they have appropriate measures in place to safeguard the personal data. All contractors should be assessed by NRS to ensure adequate security measures are in place using the Audit Security Questionnaire as a guide (see Annex C).

12.4 NRS should include a general statement in all contracts which involve the processing of personal data. It should read:

"In cases where the contractor will be processing personal data on behalf of NRS, they will be expected to sign a supplementary contract to ensure compliance with the terms of the Data Protection Act 1998."

A Data Protection Schedule should also be added to such contracts (see Annex D).

12.5 NRS should conduct regular audits of data processors to ensure contractual obligations are met.

ANNEX A: PERSONAL DATA AUDIT FORM FOR BUSINESS INFORMATION

Branch responsible for data

«Branch»

Name of collection of personal data

«Name of collection»

Description (including dates of material)

«Description»

What is the nature of the personal data?

«Nature of data»

What is the data used for?

«Use»

Who/what is the source of the data?

«Source»

Where is the data stored?

«Storage»

Who has access to the data?

«Access»

What are the security arrangements?

«security arrangements»

How long is the data kept?

«Retention period »

Is the data seen or sent outside the EEA?

«EEA»

What uses and disclosure has the data subject agreed to?

«**Uses/Disclosure**»

Is the data regularly checked for accuracy?

«YES/NO»

When was it last checked?

«Date»

ANNEX B: CCTV Access and Disclosure Form

Please use this form to report incidents which require viewing and/or disclosure of images recorded by the CCTV system operating in NRS buildings.

Requests for disclosure of CCTV footage must first be approved by the Data Protection Officer.

Police requests for access to CCTV images outside of office hours (16:30pm-9am) will be dealt with by the Accommodation Manager.

A copy of this form should be sent to the Data Protection Officer to keep on file.

Name of Reporting Officer	
Job Title	
Date of Incident (YYYY/MM/DD)	
Time of Incident (HH:MM)	
Location of Incident	
Details of Incident (provide a brief description of the incident)	
Is this a police request?	**Yes / No**
Date the Data Protection Officer / Accommodation Manager notified (YYYY/MM/DD)	
Date request to view images passed to SG Security Control Room (YYYY/MM/DD)	
Date of disclosure of images (YYYY/MM/DD)	

ANNEX C: Audit Security Questionnaire

General Procurement	Evidence	Comments
Is the data processor a reputable organisation with an established customer base?		
Are references from other clients available?		
Have checks been made to ensure that the organisation is solvent?		
Organisational security		
Does the data processor have a data protection infrastructure in place?		
Has an individual been appointed to take control of data protection responsibilities for the data processor?		
Will this individual provide a contact point for data protection enquiries from NRS?		
Has the data processor put a data protection policy in place? If so request a copy		
Is there evidence that the policy is implemented?		
What evidence can the data processor provide to demonstrate that it takes reasonable steps to ensure the reliability of staff who have access to data?		
Do all staff with access to the data controlled by NRS receive adequate levels of training in data protection?		
Can the data processor demonstrate that a breach of data protection is a disciplinary offence within the organisation?		
Are organisational measures in place to restrict access to staff without authority to process the data?		
Are provisions in place with any sub-contractors used by the data processor to ensure that similar levels of protection can be guaranteed where the sub-contractor has access to the data?		
Technical Security		
Are the automated systems used protected by a level of technical		

security appropriate to the data held?		
Are technical measures in place to restrict access to systems holding personal data?		
Are technical measures in place to secure data during transit?		
Is data stored by the data processor's subcontractors? If so can the data processor ensure that adequate technical measures are put in place by the subcontractor?		
Can both the data processors and their subcontractors demonstrate that data are backed up on a daily basis and stored in a secure site?		
Physical Security		
Are the premises on which the data are to be held secure?		
Is access to those premises restricted?		
Are the premises subject to 24 hour security?		
Are the premises monitored by CCTV?		
Within the premises are the areas where the data are to be held secure?		
If the data are held on a non-automated system, is access still restricted – for example locked cabinets, clear desk policy?		
Are any copies of data, print outs, obsolete back ups, etc disposed of securely?		
Are obsolete hardware and software from which data could be discovered disposed of securely?		
Is there an auditable data retention and destruction policy?		

ANNEX D: Data Protection Schedule

The Data Controller and the Data Processor HAVE AGREED on the following clauses('the Clauses') in order to adduce to adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data controller to the data processor of the personal data specified in Appendix 1.

1. DEFINITIONS

1.1 For the purposes of the Clauses:

'personal data'; means data which relate to a living individual who can be identified-
(a) from those data, or
(b) from those data and other information which is in the possession of, or likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

'sensitive personal data'; means personal data consisting of information as to –
(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union,
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or sentence of any court in such proceedings;

'process/processing'; in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including –
(a) organisation, adaptation, or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) alignment, combination, blocking, erasure or destruction of the information or data;

'Data Controller' means a person who (either jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;

'Data Processor'; means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;

'Data Subject'; means an individual who is the subject of personal data;

'supervisory authority'; means the Office of the Information Commissioner.

'The Act'; means the UK Data Protection Act 1998.

2. DETAILS OF TRANSFER

2.1 The details of transfer, and in particular the categories of personal data the purposes for which they are transferred, are specified in Appendix 1 which forms an integral part of the Clauses.

3. THIRD-PARTY BENEFICIARY CLAUSE

3.1 The data subjects can enforce this Clause, Clause 4(b), (c) and (d), Clause 5 (a), (b), (c) and (e), Clause 6 (1) and (2) and Clauses 7,9 and 11 as third party beneficiaries.

3.2 The parties do not object to the data subjects being represented by an association or other bodies if they so wish and if permitted by national law.

4. OBLIGATIONS OF THE DATA CONTROLLER

4.1 The data controller agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data by him,, has been and, up to the moment of transfer, will continue to be carried out in accordance with the relevant provisions of the Act.

(b) that if the transfer involves sensitive personal data the data subject has been informed or will be informed before the transfer that this data could be transmitted to a data processor.

(c) to make available to the data subjects upon request a copy of the Clauses; and

(d) to respond in reasonable time and to the extent reasonably possible to enquiries from the supervisory authority on the processing of the relevant personal data by the data processor and to any enquiries from the data subject concerning the processing of this personal data by the data processor.

5. OBLIGATIONS OF THE DATA PROCESSOR

5.1 The data processor agrees and warrants:

(a) that he has no reason to believe that the legislation applicable to him prevents him from fulfilling his obligations under the contract and that in the event of a change in that legislation which is likely to have substantial adverse effect on the guarantees provided by the Clauses, he will notify the change to the data controller and to the supervisory authority where the data controller is established, in which case the data controller is entitled to suspend the transfer of data and/ or terminate the contract;

(b) to process the personal data in accordance with the mandatory data protection principles set out in Appendix 2;

(c) to deal promptly and properly with all reasonable inquiries from the data controller or the data subject relating to the processing of the personal data subject to the transfer and to cooperate with the competent supervisory authority in the course of all its inquiries and abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(d) at the request of the data controller to submit its data processing facilities for audit which shall be carried out by the data controller or an inspection body composed of independent members and in possession of the required professional qualifications, selected by the data controller, where applicable , in agreement wit the supervisory authority;

(e) to make available to the data subject upon request a copy of the Clauses and indicate the office which handles complaints.

6. LIABILITY

6.1 The parties agree that a data subject who has suffered damage as a result of any violation of the provision referred to in Clause 3 is entitled to receive compensation from the parties for the damage suffered. The parties agree that they may be exempted from this liability only if they prove that neither of them is responsible for the violation of those provisions.

6.2 The data controller and the data processor agree that they will be jointly and severally liable for damage to the data subject resulting from any violation referred to in paragraph 1. In the event of such a violation, the data subject may bring an action before a court against either the data controller or the data processor or both.

7. MEDIATION AND JURISDICTION

7.1 The parties agree that if there is a dispute between a data subject and either party which is not amicably resolved and the data subject invokes the third-party beneficiary provision in Clause 3, they accept the decision of the data subject:
(a) to refer the dispute to mediation by an independent person, or, where applicable, by the supervisory authority;
(b) to refer the dispute to the courts.

7.2 The parties agree that by agreement between a data subject and the relevant party a dispute can be referred to an arbitration boy, if that party is established in a country which has ratified the New York convention on enforcement or arbitration awards.

7.3 The parties agree that paragraphs 1 and 2 apply without prejudice to the data subject's substantive or procedural rights to seek remedies in accordance with the other provisions of national or international law

8. COOPERATION WITH SUPERVISORY AUTHORITIES

8.1 The parties agree to deposit a copy of this contract with the supervisory authority if it so requests.

9. TERMINATION OF THE CLAUSES

9.1 The parties agree that the termination of the clauses at any time, in any circumstance and for whatever reason does not exempt them from obligations and/or conditions under the Clauses as regards the processing of the data transferred.

10. VARIATION OF THE CONTRACT

10.1 The parties undertake not to vary or modify the terms of the clauses.

APPENDIX 1

To the standard contractual clauses

This appendix forms part of the clauses and must be completed and signed by the parties

Data Controller
The data controller is (specify your activities relevant to transfer)
……
……
……
……

Data Processor
The Data Processor is (specify your activities relevant to the transfer)
……
……
……
……

Data Subjects
The personal data transferred concern the following categories of data subject (be specific)
……
……
……
……

Purposes of transfer
The transfer is necessary for the following purposes (please specify)
……
……
……
……

Categories of data
The personal data transferred will fall within the following categories of data (please specify)
……
……
……
……

Sensitive data
The personal data transferred fall within the following categories of sensitive data (please specify)
……
……
……
……

Recipients
The personal data transferred may be disclosed only to the following recipients or categories of recipients, (please specify)

……
……
……
……