Data Protection Policy

RSM Medicals Limited (the “Company”) Data Protection Policy specifies the steps which the Company is taking to conform to the requirements of the Data Protection Act.

- Scope and Status
- Definitions
- Data Protection Act Overview
- Staff Responsibilities
- Gathering Data
- Privacy Policy Relating to the Company Website
- Disclosure of Data
- Transfer Outside the EEA
- Publication of Data
- Security of Data
- Use of Data in Research
- References and Recruitment
- Retaining Data
- Records Management
- Access to Data
- Data Protection Contacts

1. Scope of the Policy

The Company needs to collect certain types of personal information about the people with whom it deals, such as donors selected for drug and alcohol testing, medicals and students attending training courses, and those with whom it communicates. This information has to be collected for administrative purposes, and to fulfil legal obligations as prescribed to ensure chain of custody requirements have been met. The Data Protection Act 2018 requires that this information should be processed fairly, stored safely and not disclosed to any other person unlawfully. The Company is committed to protecting the rights and privacy of individuals in accordance with the requirements of the Data Protection Act. This document outlines The Company's policies in relation to the Data Protection Act.

The Company's Data Protection Policy applies to all donors, students and staff of the Company. Any breach of the policy may result in The Company, as the registered data controller, being liable in law for the consequences of the breach. Legal liability may also extend to the individual processing the data and his/her Head of Department or line manager under certain

circumstances. In addition, breach of The Company's Data Protection Policy by staff will be considered to be a disciplinary offence and will be dealt with according to the Company's disciplinary procedures. Any member of staff, donor or student who considers that the policy has not been followed with respect to personal data about themselves should raise the matter with The Company's Information Compliance Manager (see Data Protection contacts).

This policy applies to all personal data for which the Company is responsible, including electronic data and manual data which are covered by the Data Protection Act (see Overview of the Data Protection Act 2018). It applies regardless of where the data are held, and regardless of the ownership of the equipment used for processing, if the processing is performed for the Company purposes. Outside agencies and individuals who work with the Company, and who have access to personal information for which the Company is responsible, will be expected to comply with this policy and with the Data Protection Act.

2. Status of the Policy
This policy statement has been adopted by the Company and was reviewed and approved by the Company's Director and Senior Management during early February 2023.

Definitions

This page explains terms which are commonly used in the Data Protection Policy.

Data controller
A person or organisation who makes decisions in regard to personal data, including decisions regarding the purposes for which and the manner in which personal data may be processed.

Data processor
An individual or organisation other than an employee of the data controller, who processes personal data on behalf of the data controller: e.g. a firm which collects and processes data on the Company's behalf under contract. Data controllers are responsible for the processing, which is carried out for them by data processors, and have to ensure that this processing takes place within appropriate security arrangements (see Security of data).

Data subject
A living individual who is the subject of personal data.

Direct marketing
The communication of advertising or marketing material directed to particular individuals.

Manual data
Personal data which are not being processed by equipment operating automatically or recorded with the intention that they should be processed by such equipment: e.g. data held in paper form.

Personal data
Data relating to a living individual who can be identified from the data, or from the data and other information which is in the possession of (or likely to come into the possession of) the data controller. Personal data may include information such as an individual's name, home and work addresses, medical history, educational background, images and photographs, expressions of opinion about the individual, and the intentions of the data controller in regard to the individual.

Processing
Any operation on personal data, including obtaining, recording, holding, organizing, adapting, combining, altering, retrieving, consulting, disclosing, disseminating, deleting, destroying and otherwise using the data.

Relevant filing system
A filing system for paper or other manual data which has been constructed in such a way that specific categories of information relating to an individual are readily accessible.

Sensitive personal data
Personal data relating to racial or ethnic origins, political opinions, religious beliefs, trade union membership, physical or mental health (including disabilities), sexual life, the commission or alleged commission of offences, and criminal proceedings.

Third parties
An individual or organisation other than the data subject, the data controller or a data processor acting on behalf of the data controller.

Vital interests
Although not defined in the Data Protection Act, the Information Commissioner has advised that "vital interests" should be interpreted as relating to life and death situations: e.g. the disclosure of a data subject's medical details to a hospital casualty department after a serious accident.

Overview of the Data Protection Act 2018

The Data Protection Act 2018 commenced on 23rd May 2018, with specific sections relating to the General Data Protection Regulations (GDPR). It replaced and broadened the Data Protection Act 1988. The purpose of the Act is to protect the rights and privacy of individuals, and to ensure that data about them are not processed without their knowledge and are processed with their consent wherever possible. The Act covers personal data relating to living individuals, and defines a category of sensitive personal data which are subject to more stringent conditions on their processing than other personal data.
The Data Protection Act covers data held in electronic formats, and also applies to manual data which are held in what the Act calls a relevant filing system. While this might appear to limit the categories of non-electronic data to which the Act applies, the definitions of personal data in the Data Protection Act have been broadened by the Freedom of Information Act 2000 in respect of public authorities. The main effect of this is that since 1 January 2005 (when the Freedom of Information Act came into force), unstructured personal information held in manual form - i.e. not in a relevant filing system - is covered by the Data Protection Act, except for unstructured data relating to appointments, removals, pay, discipline and other personnel matters, which remain outside the scope of the Act.
It should therefore be assumed, as a general rule, that any personal data relating to an identifiable living individual which are held by the Company in any form are covered by the Data Protection Act. However, unstructured manual data are exempt from many aspects of the Act, including the first, second, third, fifth, seventh and eighth Data Protection Principles, and from the sixth Data Protection Principle except in regard to the rights of data subjects to have access to their data and to require the rectification, blocking, erasure or destruction of inaccurate data. Further information about the Data Protection Principles is provided below.
The Company is a data controller in respect of the data for which it is responsible. This means that the Company is responsible under the Data Protection Act for decisions in regard to the processing of personal data, including the decisions and actions of external data processors acting on the Company's behalf. The Data Protection Act requires that processing

should be carried out according to eight Data Protection Principles. These are outlined below, together with the Company's commitments to upholding these principles:

Data Protection Principles

(1) Personal data shall be processed fairly and lawfully.

The Company will ensure that data are obtained fairly, and will make reasonable efforts to ensure that data subjects are told who the data controller is, what the data will be used for, for how long the data will be kept and any third parties to whom the data will be disclosed. In order for processing to be fair and lawful, data which is not sensitive personal data will only be processed by the Company if at least one of the following conditions, set down in the Data Protection Act, has been met:

1. The data subject has given his/her consent to the processing.
2. The processing is necessary for the performance of a contract with the data subject, or for taking steps with a view towards entering into a contract.
3. The processing is required under a legal obligation other than a contract.
4. The processing is necessary to protect the vital interests of the data subject.
5. The processing is necessary for the administration of justice, the exercise of functions under an enactment, the exercise of functions of the Crown or a government department, or any other functions of a public nature exercised in the public interest.
6. The processing is necessary to pursue the legitimate interests of the Company or of third parties, and does not prejudice the rights, freedoms or legitimate interests of the data subject.

Processing of sensitive personal data is subject to more stringent restrictions under the Data Protection Act. Processing of sensitive personal data will only be carried out by the Company if at least one of the above conditions, applicable to non-sensitive data, has been met. In addition, at least one of the following conditions, set down in the Data Protection legislation, must also be met:

1. The data subject has given his/her explicit consent.
2. The processing is required by law in connection with employment.
3. The processing is necessary to protect the vital interests of the data subject or another person.
4. The information has been made public by the data subject.
5. The processing is necessary for legal proceedings, obtaining legal advice, or establishing or defending legal rights.
6. The processing is required for the administration of justice, the exercise of functions under an enactment, or the exercise of functions of the Crown or a government department.
7. The processing is necessary for medical purposes and is carried out by a health professional or a person with an equivalent duty of confidentiality.
8. The processing is necessary to trace equality of opportunity between people of different racial or ethnic backgrounds, different religious beliefs, or different states of physical or mental health or physical or mental conditions.
9. The processing is in the substantial public interest, and is necessary for preventing or detecting any unlawful act or failure to act.
10. The processing is in the substantial public interest, and is necessary for the protection of the public against dishonesty, malpractice, unfitness, incompetence, seriously improper conduct, mismanagement in the administration of services or failure in services.
11. The processing is in the substantial public interest, and involves the publication of information relating to point (10) or publication for the purposes of journalism, literature or art.

12. The processing is in the substantial public interest, and is necessary for the functions of a counselling service.
13. The processing is in the substantial public interest, and is necessary for research purposes; provided that the processing will not support measures or decisions with regard to individuals, and will not cause substantial damage or distress to the data subject or any other person.

This list omits some conditions relating to the processing of sensitive personal data which are unlikely to be relevant to the Company.

Data relating to the disabilities of donors, students, staff and other individuals are sensitive personal data under the Data Protection Act. Such data must be processed in accordance with the Company's Disability Policy.

(2) Personal data shall be obtained only for a specified and lawful purpose or purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.
The Company will ensure that data which are obtained for a specified purpose are not used for a different purpose, unless that use is done with the consent of the data subject, is covered by the Company's registration with the Information Commissioner, or is otherwise permitted under the Data Protection Act.

(3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
The Company will not collect personal data which are not strictly necessary for the purpose or purposes for which they were obtained.

(4) Personal data shall be accurate and, where necessary, kept up to date.
The Company will take reasonable steps to ensure the accuracy of personal data which it holds, and will take steps to correct inaccurate data when requested to do so by a data subject.

(5) Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
The Company will ensure that personal data are not kept for longer than is required by the purpose or purposes for which the data were gathered. The Company may retain certain data indefinitely for research purposes (including historical or statistical purposes), as permitted under the Data Protection Act, subject to the conditions laid down in the Act for this type of processing (see Use of personal data in research).

(6) Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.
The Company will ensure that personal data are processed in accordance with the rights of data subjects under the Data Protection Act. These rights include the right to:

- Make subject access requests (see Access to data) to find out what information is held about them, the purposes for which it will be used, and to whom it has been disclosed.
- Prevent the processing of data which is likely to cause them substantial damage or substantial distress.
- Prevent processing for the purposes of direct marketing.
- Be informed about automated decision-making processes that affect them.
- Prevent significant decisions that affect them from being made solely by automated processes.
- Sue for compensation if they suffer damage through contravention of the Act.

- Take action to require the rectification, blocking, erasure or destruction of inaccurate data.
- Request an assessment by the Information Commissioner of the legality of any processing that is occurring.

(7) Appropriate technical and organisational measures shall be taken to prevent the unauthorised or unlawful processing of personal data and the accidental loss, destruction of or damage to personal data.
The Company will take steps to ensure the security of personal data which are held electronically and in manual form, to prevent the unauthorized disclosure of data to third parties, and loss or damage to data that may affect the interests of data subjects. The Company will also ensure that data processors provide an appropriate level of security for the personal data which they are processing on the Company's behalf (see Security of data).

(8) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
The Company will not transfer data outside the European Economic Area unless the transfer would be permitted under the Data Protection Act (see Transferring data outside the EEA).
The Data Protection Act requires bodies which record and use personal information to register with the Information Commissioner. The Company's registration details are included in the Register of Data Controllers which is available on the website of the Information Commissioner. It records the purposes for which the Company gathers personal data, the types of data subjects covered by each purpose, the classes of data gathered, recipients to whom the data will be disclosed, and countries or territories to which the data may be transferred. Any use by the Company of personal data must be in accordance with the terms of the Company's registration.

Further information about the Data Protection Act is available on the website of the Information Commissioner. Members of the Company may also wish to consult the Data Protection Code of Practice for the HE and FE Sectors which has been prepared by the Joint Information Systems Committee (JISC), and the Data Protection resources published by the JISC Legal Information Service.

General Responsibilities of the Company Staff

The Company as a corporate body is a data controller under the Data Protection Act. The Company's Information Compliance Manager has oversight of planning and policy development matters in the area of information compliance, including Data Protection.

When processing personal data, the Company staff must ensure that they abide by the Data Protection Act, this policy and any related policies (see Related guidelines and policies). The Company must only process personal data in accordance with its registration with the Information Commissioner. The registration defines, in a very general way, the purposes for which the Company processes personal data and related information (see Data Protection Act Overview), and is available on the Information Commissioner's website as part of the Register of Data Controllers. In practice, most routine uses of personal data will be covered by the Company's registration and will be legitimate from a Data Protection standpoint. However, this will not necessarily be the case where changes are introduced to the way in which data are processed - such as using the data for a purpose for which the data have not previously been used or transferring the data to a new source.

Before such changes are introduced, staff should check to ensure that the proposed changes will be in accordance with the Company's registration with the Information Commissioner, and will comply with the Data Protection Act and this Policy. Staff who are uncertain as to whether their

processing of data meets these requirements should refer any queries to the Company's Information Compliance Manager in the first instance. Staff should also ensure that any personal information for which they are responsible is accurate and up to date, including information which the Company holds about themselves (e.g. their home address), and that data for which they are responsible are kept secure and are not disclosed to unauthorised parties (see Security of Data).

Data should only be transferred internally within the Company when there is a genuine business need to do so. Staff who receive transferred data are equally responsible for ensuring that the data are processed in accordance with this policy and the Company's obligations under the Data Protection Act. It is important that internally transferred data should continue to be used for purposes which are consistent with the purposes which applied when the data was gathered, to avoid violation of the second Data Protection Principle (see Data Protection Act Overview). Particular care should be taken when disclosing personal data to parties outside of the Company (see Disclosure of Data).

The Company's Information Compliance Manager is responsible for ensuring that the processing of personal data at the Company conforms to the requirements of the Data Protection Act and this policy. In particular, he/she should ensure that new and existing staff who are likely to process personal data are aware of their responsibilities under the Act. This includes drawing the attention of staff to the requirements of this policy, and ensuring that staff who have responsibility for handling personal data are provided with adequate training. This includes establishing retention periods to ensure that personal data are not kept for longer than is required (see Retaining Data).

Staff should also note that the Company is not responsible for any processing of personal data by them which is not related to their employment with the Company, even if the processing is carried out using the Company's equipment and facilities. Staff are personally responsible for complying with the Data Protection Act in regard to data for which they are the data controller.

Gathering Data

Any gathering of personal data by members of the Company must be accordance with the Company's registration with the Information Commissioner (see Data Protection Act Overview). Staff should check the Register of Data Controllers on the Commissioner's website (or consult with the Information Compliance Manager) before introducing any new form of data gathering or making changes to existing methods of data gathering. If it appears that the collection of the data would not be covered by the Company's existing registration, the Information Compliance Manager must be informed before the changes are implemented, so that the Company's register entry can be updated (see Data Protection Contacts).
While it is not always necessary to have the consent of the data subject in order for the processing of data to be fair and lawful, it is advisable to seek consent wherever possible, particularly in regard to sensitive personal data where explicit consent should normally be obtained (see the discussion of the first Data Protection Principle in Data Protection Act Overview). The Company also has a general obligation under the first Data Protection Principle to ensure that data subjects are provided with information about how their data will be used by the Company, unless doing so would involve disproportionate effort. To meet these requirements, paper and electronic forms (including web based forms) created by the Company which gather personal data should always include a fair processing notice.
It is recommended that fair processing notices used on the Company forms should explain:

- Why the data needs to be gathered and how the data will be used **[essential]**.
- The parts of the Company that will use the data **[desirable]**.
- Any third parties outside the Company to whom the data will be disclosed or transferred **[essential]**.

- How long the data will be kept **[desirable]**.
- The fact that completion of the form will be taken as consent by the data subject to the use of the data as outlined **[essential]**.
- How the data subject can exercise his/her rights under the Data Protection Act (e.g. by linking to the Company's Data Protection web pages or by providing contact details for the Company's Information Compliance Manager) **[desirable]**.

To avoid infringement of the third Data Protection Principle, forms and other methods of data collection should not gather more data than are necessary for the task at hand. Staff who are responsible for the design of forms should ensure that there is a clear business need for each data item requested. Otherwise, the form should be amended to remove the data item.

Data subjects have the right to prevent the processing of their data for direct marketing purposes (e.g. promotional mail shots). If personal data gathered via a form is to be used for direct marketing, the form must also include:

- A statement explaining how the data will be used for direct marketing.
- Information on how the data subject can opt out of the use of the data for that purpose (e.g. by ticking a box).

Where direct marketing is involved, the form should indicate that it is assumed that the data subject consents to the use of the data for direct marketing purposes unless he/she specifies otherwise.

Information about visitors to a website gathered through cookies, web bugs and other devices will become personal data if the data is linked to personal details of the user, such as name and address details submitted through an online form. The Company's website which use cookies, web bugs and other tracking devices in this way should include a privacy statement explaining:

- Which data will be collected in this way.
- Which parts of the Company will use the data.
- How the data will be used.
- How long the data will be kept.
- How users can disable cookies, web bugs and other devices if they wish to do so.

Privacy policy relating to the Company website

In this agreement, the "Website" means the Company website at www.rsmtests.co.uk.

The Company is committed to protecting your privacy and developing technology that gives you a safe online experience. This Privacy Policy applies to the Website and governs data collection and usage. By using the Website, you consent to the data practices described in this policy.

The Website is operated by RSM Medicals Ltd. (called the Company in this agreement), who are situated at Olympic House, 28-42 Clements Road, Ilford, Essex IG1 1BA. The Company can be contacted by post to Olympic House, 28-42 Clements Road, Ilford, Essex IG1 1BA. You can reach us by telephone at 020 3930 8983.
The Company encourages you to review the privacy statement of websites you choose to link to from the Website so that you can understand how those websites collect, use and share your information. Any third-party sites that you can access through the Website are not covered by The Company's Privacy Policy and we accept no responsibility or liability for these sites.

Information you give us

We receive and store any information you enter on the Website or give us in any other way. You provide this information when you search, participate in discussion forums or communicate with us by phone, email or otherwise. As a result of those actions you might supply us with such information as your name, address, post code, date of birth, gender, information on how you use our services (such as type, date, time, and information on your browsing activity when visiting the Website) and any other information with respect of your use of the Website. We might also ask for other specific information from time to time.

We use the information that you provide for such purposes as responding to your requests, customising future use of the Website for you, improving the Website and communicating with you.

Automatic information

We receive and store certain types of information whenever you interact with us. For example, like many websites, we use "cookies" and "webbugs", and we obtain certain types of information when your web browser accesses the Website. Third parties might also do this on the Website. Examples of information we collect and analyse using technology which is not readily apparent include the Internet Protocol (IP) address used to connect your computer to the internet; log in; email address; password; computer and connection information such as browser type and version, operating system and platform; the full Uniform Resource Locators (URL), click stream to, through and from the Website, including date and time; cookie number; pages viewed or searched for; your site history, and phone number used to contact us. A number of companies offer utilities designed to help you visit websites anonymously. We want you to be aware that these tools exist.

What are Cookies and Webbugs?

- Cookies are pieces of information that we transfer to your computer's hard drive through your web browser when you are viewing the Website. These pieces of information allow the Website to act on information that will make your use of the Website more rewarding. We use cookies to enable our system to recognise your browser and to provide features such as easier login and greater security and for storing information about you between visits. None of these cookies contain your password, phone number or address details in text format.
- The "help" portion of a toolbar on most browsers will tell you how to protect your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. However if you turn cookies off you won't have access to some of the features that make the Website more efficient and services may not function properly.

- Web bugs are minute images (commonly 1 pixel x 1 pixel to be exact) that transmit data on use of the internet back to a computer specified by the web bug. Information fed back by web bugs is often similar to the sort of information you will find in a cookie, such as the sites that you have recently visited and potentially the characteristics of the machine that you were using.

Does RSM Medicals Ltd. share the information received?

The Company collects and uses your personal information to operate the Company and deliver any services you have requested.

The Company does not use or disclose sensitive personal information, such as race, religion or political affiliations, without your explicit consent, and would not normally gather this information in the course of your day to day use of the website.

RSM Medicals Ltd. may disclose personal information in the following circumstances:

- We may pass personal data to other organizations within or outside the European Economic Area who are contracted to provide services to the Company, where the transfer is necessary for the provision of those services. The Company is responsible under the Data Protection Act for the data processing carried out by these organizations.
- The Company may share data with trusted partners to help us perform statistical analysis, or anonymously as part of a research paper. All such third parties are prohibited from using your personal information except to provide these services to the Company, and they are required to maintain the confidentiality of your information.
- We may provide your data to third parties where we have informed you in advance that we will do so and have obtained your permission.
- We will give out personal information as required or permitted by law, for example to comply with a Court Order, to enforce our terms and conditions or to protect the safety and security of users on the Website.

We may use the data which you provide for direct marketing purposes (e.g. to send you emails or postal mail). We will tell you at the point of gathering the data whether your data is to be used for direct marketing purposes. You may request at any time that we not use your data for these purposes.

How secure is information about me?

- The importance of security for all personally identifiable information associated with our users is of utmost concern to us. We take technical, contractual, administrative and physical steps to protect all of the user information we hold. Despite this no system is 100% secure and you acknowledge that the information you give us is at risk.
- It is important for you to protect against unauthorised access to your password and to your computer. Be sure to log out when using a shared computer and take steps to make sure your personal information has not been stored by that computer or a network connected to it.

What choices do I have?

- The help portion of the toolbar on most browsers will tell you how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie or how to disable cookies altogether.
- You can visit sites on the internet that will tell you more about webbugs and what to do about them.
- There are products which allow anonymous browsing.

Conditions of use

This agreement is governed by the laws of England, where the Company originates and is designed to be accessed and is deemed to be made in England. You consent to the exclusive jurisdiction of the English courts in all disputes arising out of or relating to the use of the Website. Use of the Website is unauthorised in any jurisdiction that does not give effect to all provisions of these terms and conditions, including without limitation this paragraph.

By continuing to use the Website you agree that you have read the Access Agreement and that you agree with all of its contents. This agreement and the Access Agreement may be altered and for this reason you should regularly visit the Privacy Policy on the Website as the current version will be binding upon you.

Further information

The Company's website is operated in accordance with the Company's Data Protection Policy, which provides further information about the steps taken by the Company to comply with the Data Protection Act.

1.1.1 Disclosure of Data

Staff must take particular care when disclosing personal data to third parties, to ensure that there is no breach of the Data Protection Act or the law of confidence.

Disclosure may be unlawful even if the third party is a family member of the data subject, or a local authority, government department or the police. A key point to consider is whether the disclosure is relevant to and necessary for the conduct of the Company's business. For example, it would generally be appropriate to disclose a staff member's work contact details in response to an enquiry relating to a function for which they are responsible, but it would not be reasonable or appropriate to disclose a staff member's personal address or bank account details.

The disclosure of personal data represents a form of processing of the data. This means that the conditions for fair and lawful processing of personal data and sensitive personal data set out in first Data Protection Principle must be met (see Data Protection Act Overview). Consideration should also be given as to whether the disclosure was one of the purposes for which the data were originally gathered; in particular, whether the disclosure is covered by the Company's entry in the Information Commissioner's Register of Data Controllers, or is a purpose to which the data subject has consented. If not, the disclosure is likely to represent further processing contrary to the second Data Protection Principle.

Disclosure of personal data which are not sensitive personal data is most likely to be justified if one or more of the following conditions applies:

- The data subject has given his/her consent to the disclosure (e.g. at the time when the data were gathered).
- The disclosure is in the legitimate interests of the Company or of the third party to whom the data are to be disclosed, and does not prejudice the rights, freedoms or legitimate interests of the data subject.
- There is a statutory or legal obligation to disclose the data.
- The disclosure is required for the performance of a contract.
- The disclosure is necessary to protect the vital interests of the data subject.

More stringent restrictions apply to the processing of sensitive personal data (see Data Protection Act Overview). The most likely conditions that would justify disclosure of sensitive personal data are:

- The data subject has given his/her explicit (ideally written) consent to the disclosure, or
- There is a statutory or legal obligation to disclose the data, or]
- The disclosure is necessary to protect the vital interests of the data subject.

The Data Protection Act also allows personal data to be disclosed to third parties without the consent of the data subject, in the following circumstances:

- The disclosure is necessary for safeguarding national security.
- The disclosure is necessary for the prevention or detection of crime, or the apprehension or prosecution of offenders.
- The disclosure is necessary for the assessment or collection of any tax or duty.
- The disclosure is necessary for the discharge of regulatory functions (including the health, safety and welfare of people at work).
- The data to be disclosed are to be used for research purposes, subject to the rules governing the Use of Data in Research.
- The data are information which the Company is obliged by legislation to provide to the public.
- The disclosure of the data is required by legislation, rule of law or the order of a court.

Staff should always exercise caution when dealing with requests from third parties for the disclosure of personal data. Disclosure requests should normally be required to be in writing, and should be responded to in writing. Where reasonable, the party making the request should be required to provide a statement explaining the purpose for which the data is requested, the length of time for which the data will be held, and an undertaking that the data will be held and processed according to the Data Protection Principles. Where the request relates to the prevention/detection of crime, the apprehension/prosecution of offenders, assessment/collection of any tax or duty, or the discharge of regulatory functions, appropriate paperwork should be produced by the enquirer to support their request (e.g. official documentation stating that the information is required in support of an ongoing investigation).

Personal data should only be disclosed over the telephone in emergencies, where the health or welfare of the data subject would be at stake. If data have to be disclosed by telephone, it is good practice to ask the enquirer for their number and to call them back. Particular care should be taken when dealing with requests from embassies and high commissions, as data subjects may choose to have little or no contact with representatives of their home states. Similarly, members of the Company may have reasons for not wanting contact with parents, other relatives or friends. Requests from relatives, friends etc for the contact details of donors, staff and/or students should therefore be treated with caution. It is good practice to offer to pass on any message without providing contact details or confirming or denying that the person is a member of the Company.

An image of an identifiable individual is personal data about them. In some situations, publication of an image without the individual's permission will infringe their right to privacy and the Data Protection Act. Staff involved in publishing images on the Company website should consult the Company Information Compliance Manager for guidance on appropriate safeguards for the publication of images of individuals.

Transfer Outside the EEA

The eighth Data Protection Principle (see Data Protection Act Overview) requires that personal data must not be transferred outside the European Economic Area (the European Union member states plus Iceland, Norway and Liechtenstein), unless the country or territory to which the data are to be transferred provides an adequate level of protection for personal data.
The European Commission has recognised a number of non-EEA countries which it deems to provide an adequate level of protection for personal data. Transfer of data to these countries will not violate the eighth Data Protection Principle. Similarly, the eighth Data Protection Principle will not be violated if transfer occurs in the following circumstances:

- The data is transferred to a company in the United States which has signed up to the 'Safe Harbour' agreement (a set of rules similar to those found in the UK's data protection law).
- The transfer is made under a contract which includes the model clauses adopted by the European Commission to ensure that there will be adequate safeguards for data transferred to a source outside the EEA.

Further information about the EC's list of approved countries, the 'Safe Harbour' agreement and the EC's model contractual clauses is available on the website of the Information Commissioner. The Data Protection Act also contains a number of exemptions to the eighth Data Protection Principle. The transfer of personal data outside the EEA is permitted (regardless of the country to which the data are transferred or the receiving organisation), where at least one of the following applies:

- The data subject has given his/her consent to the transfer.
- The transfer is necessary for the performance of a contract between the data controller and the data subject; or a contract between the data controller and a third party which has been entered into at the request of the data subject, or is in the interests of the data subject.
- The transfer is necessary for legal proceedings or defending legal rights.
- The transfer is necessary for reasons of substantial public interest.
- The transfer is necessary to protect the vital interests of the data subject.
- The transfer is part of the personal data on a public register.

The European Court of Justice has determined that making personal data available on a website does not contravene the Data Protection rules prohibiting the transfer of data outside the EEA (ECJ Case C-101/01 Criminal proceedings against Bodil Lindqvist). However, while it may not contravene the eighth Data Protection Principle, placing personal data on the Internet must still be done in a way that complies with the other Data Protection Principles.

Publication of Data

The Company will routinely publish a number of items that include personal data. These will include staff information (such as name, department, job title, email address and telephone number) in the Company Calendar, the Company Directory and the Company website; annual reports, staff newsletters, e-bulletins, guides, etc.

Any individual who has good reason for wishing their details in such publications to remain confidential should contact the Company's Information Compliance Manager (see Data Protection Contacts).
Staff involved in putting images on the website should also consult the Company's Information Compliance Manager, for guidance on good practice in relation to the publication of images of individuals.

Security of Data

The seventh Data Protection Principle (see Data Protection Act Overview) requires that precautions should be taken against the physical loss or damage of personal data, and that access to and disclosure of personal data should be restricted. Members of the Company who are responsible for processing personal data must ensure that personal data are kept securely, and that personal information is not disclosed orally or in writing, by accident or otherwise, to unauthorised third parties.

All Company personnel to adhere to a strict "Clean Desk" policy at the London Head Office.

Information security is a large area, so the following recommendations are meant as general guidance only. They apply equally to data processed off-site (e.g. by staff at home or on laptops), as to data processed on the Company premises. In fact, off-site processing presents a potentially greater risk of accidental loss, theft or damage to data.

Manual data

- When not in use, files containing personal data will be kept in locked stores or cabinets to which only authorised the Company staff have access. Examples of types of manual data retained are:
    - Copies of relevant passport pages
    - Copy of driving licence
    - Medical assessment records
    - Bank details
    - Sentinel card details
    - **Network Rail Training Material**
- Forms detailing name, address, NINO, contact details (telephone/email)
- Procedures for booking files in and out of storage will be developed, so that file movements can be tracked.
- Files will be put away in secure storage at the end of the working day, and will not be left on desks overnight.

Electronic data

Care must be taken to ensure that PCs and terminals on which personal data are processed are not visible to unauthorised persons, especially in public places. Screens on which personal data are displayed should not be left unattended. Particular care must be taken when transmitting personal data. Appropriate security precautions, such as the use of encryption and digital signatures, should be taken when sending personal data by email. Transmission of personal data by fax should generally be avoided.

As well as preventing unauthorised access, it is equally important to avoid the accidental or premature destruction of personal data which could prejudice the interests of data subjects and of the Company. To prevent the accidental loss of electronic data, members of the Company should ensure that storage of personal data in electronic form conforms to the good practice guidelines set down in the Company's Code of Practice for Electronic Data Storage, Transmission and Backup.

Personal data in both manual and electronic formats should only be destroyed in accordance with agreed retention schedules (see Retaining data). Care must be taken to ensure that appropriate security measures are in place for the disposal of personal data. Manual data should be shredded or disposed of as confidential waste, while hard drives, disks and other media containing personal data should be wiped clean (e.g. by reformatting, over-writing or degaussing) before disposal. Disposal of electronic media and equipment should be in accordance with the Company's Procedure for Disposing of Information Technology Equipment and Packaging.

The Data Protection Act lays particular obligations on data controllers to ensure that there are adequate safeguards for processing which is carried out on their behalf by data processors. Whenever personal data is to be processed by an external body acting on the Company's behalf, the Company must:

- Choose a data processor which provides sufficient guarantees in regard to its technical and organisational security measures;
- Take reasonable steps to ensure that the data processor complies with these measures, and

- Ensure that the processing takes place under a written contract which stipulates that the processor will act only on instructions from the Company, and that the processor will have security measures in place that ensure compliance with the seventh Data Protection Principle.

Use of Personal Data in Research

The Data Protection Act 2018 sets down certain exemptions which allow personal data to be used for research purposes (including historical or statistical research), where the data were originally gathered fairly and lawfully for other purposes. Data collected for one purpose or piece of research can be used for other research, and can be kept indefinitely, provided the following conditions are met:

- The data must be used solely for research purposes, and not for any other purposes (e.g. general administration) unless those purposes are the same as the purposes for which the data were gathered.
- The data must not be processed to support measures or decisions in regard to particular data subjects.
- The processing for research purposes must not cause, or be likely to cause, substantial damage or distress to data subjects. Closure of the data to outside access would be one way of helping to ensure this, as would anonymisation of research results.

Where the above conditions have been met, data retained for research purposes are exempt from subject access requests, provided the results of the research are not published in a form which identifies the data subjects. However, other aspects of the Data Protection Principles will still apply, such as the requirement to keep the data secure, and the requirement that the data should be processed fairly and lawfully (see Data Protection Act Overview).

In addition to the exemptions in the Data Protection Act, the Data Protection (Processing of Sensitive Personal Data) Order 2000 allows sensitive personal data to be retained in archives for research purposes, provided:

- The processing for research purposes is in the substantial public interest;
- The data are not used to make decisions about individuals without their consent; and
- The processing for research purposes does not cause substantial damage or distress to any person.

Confidential References and Recruitment

Confidential references for educational or employment purposes will involve the disclosure of personal information, often of a private nature. Requests for references which are received from reputable organizations and which request that the reference is returned to a recognised address can generally be taken at face value, where it is known that the individual who is the subject of the request has cited a member of the Company as a referee. However, if there is any doubt as to the validity of a reference request, staff should always check with the individual concerned to determine that they are willing for information about them to be released.

References given by a data controller are exempt from data subject access requests under the Data Protection Act (see Access to Data). In practical terms, this means that the Company is under no obligation to disclose the data contained in copies of references given by the Company staff. However, references received by a data controller are not exempt from subject access requests. This has the following implications, which should be taken into consideration by staff who are asked to provide references:

- References received by the Company from other individuals or organisations may have to be disclosed in response to subject access requests directed at the Company.
- References from the Company to other organisations may have to be disclosed by those organisations in response to subject access requests.

A reference will also contain personal data about the referee, such as the referee's name and address, and possibly confidential information about the referee or third parties. The information contained in a confidential reference need not be released if it would identify the referee, unless one of the following conditions can be satisfied:

- The referee's identity can be protected by anonymising the information.
- The referee has consented to the release of the data.
- It is reasonable in all circumstances to release the information without the referee's consent.

Guidance has been issued by the Information Commissioner on handling subject access requests for references, which emphasises that such requests should be dealt with on a case by case basis. All requests from data subjects for access to references should be referred to the Information Compliance Manager (see Data Protection Contacts).

Given the possibility that a reference may be disclosed as a result of a Data Protection Act request, referees should avoid making statements in references which cannot be supported by factual evidence.

Staff involved in recruitment and selection should be aware that information in documents such as interviewers' notes could potentially be disclosed to data subjects in response to access requests. Staff should therefore ensure that any feedback which is provided to candidates after interview is consistent with and can be supported by the documentation relating to the recruitment and selection process. Feedback should be provided in a manner which complies with the Company's Recruitment Policy, Recruitment Procedure and Best Practice Guidelines on Feedback.

Retention of Data

The Data Protection Act 2018 does not specify periods for the retention of personal data. It is left to data controllers to decide how long personal data should be retained, taking into account the Data Protection Principles (see Data Protection Act Overview), business needs and any professional guidelines. In the context of the Company, the following factors need to be taken into consideration:

- The need to balance the requirement of the fifth Data Protection Principle - that personal data should not be kept for longer than necessary - against the need to prevent the premature or accidental destruction of data which would damage the interests of data subjects, contrary to the seventh Data Protection Principle.
- The exemptions provided by the Data Protection Act which allow the permanent retention of data for historical and statistical research (see Use of Data in Research). The Company's history should not be endangered by the overzealous destruction of data that could be retained as historical archives.
- The fact that the Data Protection Act does not override provisions in other legislation (e.g. health and safety legislation) which specify retention periods for personal data.
-

A retention schedule is a device used by records managers to specify retention periods for series of paper and electronic records. The schedule will be developed as The Company's information audit progresses.

Advice on retention periods relating to personal data is available from the Information Compliance Manager (see Data Protection Contacts).

Staff should note that under the Freedom of Information Act, it is a criminal offence to deliberately alter, deface, block, erase, destroy or conceal data which has been the subject of an access request under the Data Protection Act or the Freedom of Information Act with the intention of preventing the release of the data. However, data may be amended or deleted after receipt of the access request but before disclosure of the data, if the amendment or deletion would have taken place regardless of the request (e.g. under a retention schedule).

Records Management

Effective management of paper and electronic records is essential for compliance with the Data Protection Act and other legislation, such as the Freedom of Information Act. In the context of Data Protection, good records management ensures that personal data contained in records:

- Can be located in response to subject access requests and business needs.
- Are protected from accidental loss or destruction.
- Are retained according to established retention periods (see Retaining Data).
- Are secured against unauthorised access and disclosure.
- Are preserved for future use, where necessary, in formats suitable for long-term preservation.

The Company Director and staff are responsible for ensuring the effective management of records within the Company. To assist in these functions, the Company's Information Compliance Manager and Operations Manager are developing the Company records management policies and procedures and will monitor their implementation. As guidance is developed, it will be included within the Company's Records Management Policy documentation. Advice and/or assistance on records management issues will be provided by the Information Compliance Manage and / or the Company's Operations Manager (see Data Protection Contacts).

1.1.2 Requesting Access to Data

The purposes for which the Company processes personal data and the types of data processed for each purpose have been registered with the Information Commissioner. Details of the Company's registration are contained in the Information Commissioner's Register of Data Controllers.

1. What are the rights of individuals?

The Data Protection Act gives data subjects the right of access to personal data which the Company holds about them, subject to certain exemptions (see What are the exemptions?). Anyone who wishes to exercise this right should apply in writing to the Company's Information Compliance Manager. Requests for access to personal data are known as subject access requests. This page explains how to submit a subject access request to the Company, how we will handle your request, and your right to complain if you are dissatisfied. There is no charge to the individual for each Data Protection request. Proof of identity is required to prevent the unlawful disclosure of personal data.

If you submit a subject access request to the Company, you are entitled to be told whether we hold any data about you. If we do, you also have the right:

- To be given a description of the data, the purposes for which the data are being processed, and those to whom the data may have been disclosed;
- To be given a copy of the data in an intelligible form, with any unintelligible terms explained;
- To be provided with any information available to the Company about the source of the data; and
- If you specifically request it, to be given an explanation as to how any decisions taken about you solely by automated means have been made.

These rights apply to electronic data, and to data in "manual" (i.e. non-electronic) formats subject to certain limitations. Further information about the rights of individuals under the Data Protection Act is available on the website of the Information Commissioner.

1.1.2.1.1.1 2. What are the exemptions?

The Data Protection Act includes various exemptions which specify the circumstances in which an organization can refuse to provide access to personal data. The most likely situations in which the Company could refuse a subject access request are where:

- The release of the data would jeopardize the prevention or detection of crime, or the apprehension or prosecution of offenders;
- Requested data is contained in a confidential reference provided by the Company;
- Requested data which record the Company's intentions in relation to any negotiations with you, and the release of the data would prejudice the negotiations;
- The data is covered by legal professional privilege;
- The data relates to management forecasting or management planning, and its release to you would prejudice the Company's business or activities; or
- Where requested data has been retained for the purposes of historical or statistical research, the conditions set out in the Data Protection Act for processing for research purposes have been met, and the results of the research have not been published in a way which identifies individuals.

The right of access to data in paper format is also subject to some limitations (ref: how the Freedom of Information affected Data Protection for further information).
If the Company withholds data as a result of an exemption under the Data Protection Act, we will explain why the data have been withheld and the relevant exemption, unless doing so would itself disclose information which would be subject to the exemption.

The Data Protection Act allows us to refuse to provide a copy of an individual's data if the effort in doing so would be disproportionate, or if the same or similar data have already been provided and a reasonable interval has not elapsed since that individual's previous subject access request. In addition, if the Company reasonably requires further information from an individual in order to locate the data which they have requested, and this is communicated to the individual, the Company are not required to comply with that individual's request until they have supplied the Company with the information.

We have to protect the Data Protection rights and other legal rights of other individuals when we respond to subject access requests. Information which does not relate to the individual making the request may be 'blanked out' or edited out, particularly if it relates to other individuals. Sometimes we may not be able to release data relating because doing so would also reveal

information about other persons who have not consented to their data being released, and it would not be reasonable in the circumstances to release the data without their consent. In suchcases, the individual making the request will be informed that their data has been withheld and the reasons for doing so.

1.1.2.1.1.2 3. How a request is submitted

Requests for access to personal data must be in writing. We ask that the individual making the request completes and returns the Company's Subject Access Request Form, which is designed to gather the information which we need to identify that individual, communicate with them and locate data about them. Failure to complete the form could delay processing of the request, as we may need to contact the individual for further information or clarification.
When completing the subject access request form, the individual should be as specific as possible about the information which they want access to, as this will assist us in processing their request. A general request such as "please send me all of the data which you hold about me" is likely to lead us to contact the individual for further information or clarification. The Company has the right to ask for information which we reasonably need to locate the data which has been requested, and we may not respond to a request until this information has been provided (see: What are the exemptions?).
Together with the form, the individual must submit proof of their identity. We will not begin processing a request until the proof of ID are received. We require proof of ID to ensure that we are releasing data to the correct person. The individual must supply a photocopy (not the original) of one of the following:

- The pages which identify the individual in their passport.
- The individual's driving licence.

If the individual is unable to supply any of the above, they must contact the Company's Information Compliance Manager (see Where can I get further information? for contact details).

Please send the completed subject access request form, fee and proof of identity by post to the following address:

Information Compliance Manager
Olympic House,
28-42 Clements Road,
Ilford,
Essex IG1 1BA
United Kingdom

The form, fee and proof of identity must be submitted for each subject access request.

1.1.2.1.1.3 4. What happens next?

The Company will send the individual an acknowledgement of their request as soon as possible. This will indicate the deadline by when we will send a response. We may also ask the individual to provide further information or clarification if we require it to process their request, and may contact them again for additional information or clarification if necessary.

After the Company receives a request, we must consider it and respond to it. We will respond as soon as possible, and in all cases within 40 calendar days of receipt of the request. If we reasonably require further information to locate the data which has been requested, we will inform

the individual making the request as soon as possible, and the 40 day deadline will commence from the date when we receive the information from them.

Any copies of data provided by the Company must be in permanent form. We will normally send the data on paper to the postal address specified on the subject access request form, unless we agree with the individual that the data can be supplied in a different format. The data may take the form of photocopies, printouts, transcripts or extracts, or a combination of these, depending on what is most appropriate in the circumstances.

If the Company holds no data about the individual making the request, they will be informed of this. The individual will also be informed of any cases where data about them has been withheld and the reasons for this, including the relevant exemptions (see What are the exemptions?), unless doing so would itself reveal information which would be subject to an exemption.

1.1.2.1.1.4 5. Can I appeal?

If an individual is dissatisfied with the handling of their Data Protection request, they are encouraged to contact the Information Compliance Manager in the first instance, to determine if the ICM can resolve their concerns informally. This may lead to a quicker resolution of the individual's complaint than a formal appeal.

If you remain dissatisfied after contacting the ICM, and you wish to complain, you should contact the Information Commissioner direct (see below).

You can also ask the Information Commissioner for an assessment as to whether the Company has processed your data in accordance with the Data Protection Act. The Commissioner can be contacted at the following address:

Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
United Kingdom

Further information about how to enforce your rights under the Data Protection Act is available on the Commissioner's website.

1.1.2.1.1.5 6. Can I re-use the data?

The copyright of any data which is supplied to you will be owned by the Company unless otherwise indicated. The supply of information under the Data Protection Act does not give the person who receives it an automatic right to re-use the information in a way which would infringe copyright, for example, by making multiple copies, publishing and issuing copies to the public.

Brief extracts of any material which is supplied to an individual may be reproduced under the fair dealing provisions of the Copyright, Designs and Patents Act 1988 (sections 29 and 30). More extensive re-use must only be carried out with prior written permission from the Company.

Enquiries about the re-use of material should be directed to the Company's Information Compliance Manager.

1.1.2.1.1.6 7. Where can I get further information?

Further information about how the Company aims to protect the rights of individuals under the Data Protection Act is provided in the Company's Data Protection Policy. Enquiries relating to Data Protection at the Company should be directed to the Company's Information Compliance Manager, whose contact details are below:

Information Compliance Manager
RSM Medicals Limited
Olympic House,
28-42 Clements Road,
Ilford,
Essex IG1 1BA
Telephone: +44 (0)333 003 4049
Email: info@rsmtests.co.uk

Information about your rights under the Data Protection Act and how to submit a subject access request is available on the website of the Information Commissioner. Other organisations, such as the Citizens Advice Bureau, may also be able to assist you in developing a subject access request.

1.1.3 Data Protection Contacts

Data Protection enquiries should be directed to the Company's Information Compliance Manager at the following address:

Information Compliance Manager
RSM Medicals Limited
Olympic House,
28-42 Clements Road,
Ilford,
Essex IG1 1BA
Telephone: +44 (0)333 003 4049
Email: info@rsmtests.co.uk

If you wish to submit a subject access request, see Requesting Access to Personal Data for further information about our procedures.

Guide to information requests under the Data Protection Act

For many organisations, a key problem with data protection legislation is handling requests for access to information. This guide outlines the key actions that an organisation should take when receiving a request for access to personal information.

Under section 7 of the Data Protection Act 2018 (DPA), individuals are entitled to access the information that an organisation holds about them. This is an important right in data protection legislation, but can have a significant impact on businesses. Businesses must carry out detailed searches quickly within a deadline of 40 days from receipt of the request. The searching can expand to cover emails, databases, paper records and CCTV records.

There is no charge to the individual for this request (regardless of the breadth of the access request). Although there are some exceptions to the right of access, organisations are often concerned about the disclosure of prejudicial information.

The request

Guide to information requests under the Data Protection Act

What is an individual entitled to?
An individual is only entitled to information that relates to them (their 'personal data') that the data controller holds in electronic form or in a 'relevant filing system'.

What is a 'relevant filing system'?

The Information Commissioner's guidance suggests that in most cases, paper records would amount to a relevant filing system for the purposes of the DPA if they are held in a 'sufficiently systematic, structured way'. If the paper records are held in no particular order (i.e. unstructured), they may not be subject to the right of access.

Does the organisation process personal data?
The fact that an individual is named in a document does not mean that the entire document is the individual's personal data. The leading case relating to access requests and personal data is Durant1.
Durant suggested that for information to be personal data it had to be "biographical in a significant sense" and that the individual making the request had to be the focus of the information. In Durant, information about the FSA's enquiry into Mr. Durant's complaint against Barclays bank was not data personal to Mr. Durant. This case has been followed by a number of cases in the First Tier Tribunal (Information Rights).

What form does the subject access request have to take?
There is no prescribed format for a subject access request, provided that it is in writing. A written can be received by fax, email, post and even social media (e.g. to the organisation's dedicated Facebook page or Twitter account). An organisation is not obliged to respond to a verbal request, unless it is satisfied of the person's identity.

What to do when a request is received

1. Ensure the request is logged and complied with promptly
Individuals do not have to say that they are making a subject access request or make reference to the DPA for it to be a valid request. Consequently, personnel who might receive such requests should be trained in data protection compliance so they can recognise a request for what it is and ensure it is dealt with promptly, within the statutory 40 day deadline. If an organisation does not comply with a request either promptly or fully, an individual can complain to the Information Commissioner who can take enforcement action.

2. Check that there is sufficient information to respond to the request
The organisation does not have to respond to a request until it has all of the information that it reasonably requires to respond and to be able to locate the information sought. The 40-day time limit for responding to the request will not start until this information, if requested, has been obtained. If the access request is not clear, the organisation is entitled to go back to the individual for more information.

3. Ensure that the individual making the request is entitled to the requested information
If the organisation is unsure of the identity of the requestor, it can ask them to provide evidence of their identity. Third parties, for example solicitors, can request data on someone else's behalf – although it is the responsibility of the third party to evidence their entitlement to represent the individual concerned. If an

individual is writing on behalf of a spouse, or a legal representative on behalf of their client, an organisation should not assume that the requestor has authority to act on behalf of the client/individual. The organisation

should ask for written evidence of authority. This could be through a written statement or a general power of attorney.

4. Carry out a search for the information requested
Once satisfied that it has enough information to carry out the search, the organisation should search for any relevant information which it may hold. Searches may encompass electronic documents (emails, database records etc.) and paper records (subject to the relevant filing system criteria, above). Information held by a data processor on the controller's behalf will also be subject to an access request if it relates to the individual about whom an access request has been made.

Archived, but not deleted, data should also be searched.

What exemptions may be relevant?
The DPA lists a number of exemptions to the obligation to disclose personal data. The most relevant of which are summarised below:

Exemption	Information (potentially) exempted
Confidential references	References given by the controller that are connected to actual or potential education, training or appointment of the data subject. This does not apply to references from a third party source.
Legal Privilege	Documents that are subject to legal professional privilege.
Management Forecasts	Data used for an organisation's forecast or planning (to the extent that disclosure would prejudice the organisation's ability to conduct its business).
Negotiations with the Individual	Information which relates to ongoing negotiations between the organisation and the individual requesting the information, where disclosure would prejudice those negotiations.
Prevention or detection of crime	Any information if its release would prejudice: • the prevention or detection of crime; • the apprehension or prosecution of offenders; or • the assessment or collection of any tax or duty or of any imposition of a similar nature.
Repeat requests	Identical or similar requests do not need responding to unless a reasonable time has lapsed or there is a reasonable circumstance.
Third Party Information	An organisation cannot refuse to provide access to personal data simply because the data refers to a third-party source. Instead, the organisation is required to undertake a 'balancing act' to ensure the privacy rights of the individual requesting the data and the third party included in the data are respected. Where the data includes third-party information, it may be possible to: • anonymise the data relating to the third party; • seek consent from the third party; or

- decide if the disclosure is reasonable, bearing in mind any duty of confidentiality owed to the third party as well as any statutory requirements.

The disclosure

The individual is entitled to a copy of their personal data, not a copy of the documents that contain their personal data.

The personal data disclosed needs to be provided in an 'intelligible form' – e.g. if codes have been used, a key to those codes should be provided so that the individual can understand the information. There is no requirement to make the data 'legible' or even understood by the recipient (e.g. translated into their native language).

The response letter

In addition to enclosing a copy of the applicant's personal data (where this is being disclosed), the response letter should identify in general terms:

- What personal data have been processed;
- The sources of that personal data;
- The purposes for which their personal data is processed; and
- The recipients of that personal data.

A note on automated decision-taking

Where an organisation makes decisions electronically without human intervention (e.g. automatic scoring after psychometric testing in graduate recruitment) ("automated decision taking"), an individual has the right to ask for information about that automated processing (trade-secret information is, however, exempt). Additionally, the individual can ask that the decision is re-taken without the use of electronic means. The organisation has 21 days to respond to such a request.

An example of one of the limited exemptions from these obligations is where the automated decision-taking is undertaken for the performance of a contract (for example, the scanning of job applicants' CVs) or where required by statute.

If an individual does not ask for information about automated decision taking, the organisation is not obliged to provide it.

Request for Personal Data under the Data Protection Act
Please complete sections A-C, and return this form together with your fee and proof of identity to The Company's Information Compliance Manager (see Section C for details).

A. Your Details

Surname: Forename(s):
Former surname(s) (where relevant):
Postal address:

Post code: Country:
Daytime telephone:
Email:
Date of birth (for identification purposes only):

B. Data Requested

Please describe the data which you are seeking as precisely as you can. Continue on a separate sheet if necessary:

C. Signature

I certify that I am the person named on this form and that I wish to be provided with the data which I have specified relating to myself under the Data Protection Act 2018. I will not publish any data which are supplied to me without prior permission from the Company or the copyright owner (if copyright is not owned by the Company), except where permitted by law.

Signature: Date:

Please enclose the following with this form:

1. A cheque or money order for GBP10.00 payable to RSM Medicals Limited

2. Proof of your identity. Please supply a photocopy (not originals) of one of the following (if you cannot supply any of these items, please contact the Company's Information Compliance Manager):
   - The pages which identify you in your passport.
   - Your driver's licence.

Please send your form, fee and proof of identity to:

Information Compliance Manager
RSM Medicals Limited
Olympic House
28-42 Clements Road
Ilford
Essex
IG1 1BA
Telephone: +44 (0)333 003 4049
Email: info@rsmtests.co.uk

Further information about how your request will be handled will be available on the Company website.

D. Data Protection Act Declaration

The data gathered by this form will be used to process your request for personal data under the Data Protection Act. It will be held by the Company's Information Compliance Manager, and may be transferred to other parts of the Company for the purposes of verifying your identity or processing your request for data. The data will be held for six years from the date when we responded to your request, unless your request forms part of an ongoing case, in which case the data will be kept for as long as necessary.

Staff use only

Form received	Fee received	ID received	Response sent
Date:	Date:	Date:	Date:

RSM MEDICALS LTD. DATA PROTECTION POLICY REVIEWED and APPROVED BY:

Signed Rabia Hassan Date Reviewed: February 2024

Director
RSM Medicals Limited