DATA PROTECTION POLICY: EXTERNAL

This policy gives important information about:

- the data protection principles with which SDL must comply;
- what is meant by personal information (or data) and sensitive personal information (or data);
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles; and
- where more detailed privacy information can be found, e.g. about the personal information we gather and use, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept.

1 Introduction

1.1 SDL obtains, keeps and uses personal information (also referred to as data) about job applicants, current and former employees, temporary and agency workers, contractors, interns, volunteers, apprentices, customers, clients, contractors, individuals interested in our business, and business associates for a number specific lawful purposes.

1.2 This policy sets out how we comply with our data protection obligations and seek to protect personal information. Its purpose is also to confirm to individuals that we understand and comply with the rules governing the collection, use and deletion of personal information which we process.

1.3 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information, and how (and when) we delete that information once it is no longer required.

1.4 The Compliance Team is responsible for informing and advising SDL and its staff on its data protection obligations, and for monitoring compliance with those obligations and with SDL's policies. If you have any questions or comments about the content of this policy or if you need further information, you should contact compliance@sdlgroup.co.uk.

2 Scope

2.1 This policy applies to the personal information job applicants, current and former employees, temporary and agency workers, contractors, interns, volunteers, apprentices, customers, clients, contractors, individuals interested in our business, and business associates.

2.2 We will review and update this policy regularly in accordance with our data protection obligations. It does not form part of any employee's contract of employment or any other contractual agreement with any person and we may amend, update or supplement it from time to time.

3 Definitions

criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means the individual to whom the personal information relates;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it; and
sensitive personal information	(sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

4 Data protection principles

4.1 SDL will comply with the following data protection principles when processing personal information:

4.1.1 we will process personal information lawfully, fairly and in a transparent manner;

4.1.2 we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

4.1.3 we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;

4.1.4 we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;

4.1.5 we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and

4.1.6 we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

5 Basis for processing personal information

5.1 In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

5.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:

(a) that the data subject has consented to the processing; or

(b) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) that the processing is necessary for compliance with a legal obligation to which SDL is subject; or

(d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person; or

(e) that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or

(f) that the processing is necessary for the purposes of legitimate interests of SDL or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject—see clause 5.2 below.

5.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

5.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

5.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

5.1.5 where sensitive personal information is processed, also identify a lawful special condition for processing that information (see paragraph 6.1.2 below), and document it; and

5.1.6 where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

5.2 When determining whether SDL's legitimate interests are the most appropriate basis for lawful processing, we will:

5.2.1 conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

5.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);

5.2.3 keep the LIA under review, and repeat it if circumstances change; and

5.2.4 include information about our legitimate interests in our relevant privacy notice(s).

6 Sensitive personal information

6.1 SDL may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

6.1.1 we have a lawful basis for doing so as set out in paragraph 5.1.1 above, e.g. it is necessary for the performance of the employment or other contract, to comply with SDL's legal obligations or for the purposes of SDL's legitimate interests; and

6.1.2 one of the special conditions for processing sensitive personal information applies, e.g.:

(a) the data subject has given explicit consent; or

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of SDL or the data subject; or

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent; or

(d) processing relates to personal data which are manifestly made public by the data subject; or

(e) the processing is necessary for the establishment, exercise or defence of legal claims; or

(f) the processing is necessary for reasons of substantial public interest.

6.2 Before processing any sensitive personal information, staff must notify compliance@sdlgroup.co.uk of the proposed processing, in order that the Compliance Team may assess whether the processing complies with the criteria noted above.

6.3 Sensitive personal information will not be processed until:

6.3.1 the assessment referred to in paragraph 6.2 has taken place; and

6.3.2 if possible, the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

6.4 SDL will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

6.5 SDL's relevant data protection privacy notice will set out the types of sensitive personal information that SDL processes, what it is used for and the lawful basis for the processing.

7 Criminal records information

7.1. Criminal records information will be processed in accordance with SDL's Criminal Records Information Policy.

8 Data protection impact assessments (DPIAs)

8.1 Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where SDL is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

8.1.1 whether the processing is necessary and proportionate in relation to its purpose;

8.1.2 the risks to individuals; and

8.1.3 what measures can be put in place to address those risks and protect personal information.

9 Documentation and records

9.1 We will keep written records of processing activities including:

9.1.1 the purposes of the processing;

9.1.2 a description of the categories of individuals and categories of personal data;

9.1.3 categories of recipients of personal data;

9.1.4 where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;

9.1.5 where possible, retention schedules; and

9.1.6 where possible, a description of technical and organisational security measures.

9.2 As part of our record of processing activities we document:

9.2.1 information required for privacy notices;

9.2.2 records of consent if necessary;

9.2.3 controller-processor contracts;

9.2.4 the location of personal information;

9.2.5 DPIAs; and

9.2.6 records of data breaches.

9.3 If we process sensitive personal information or criminal records information, we will keep written records of:

9.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

9.3.2 the lawful basis for our processing; and

9.3.3 whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

9.4 We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:

9.4.1 carrying out information audits to update what personal information SDL holds;

9.4.2 distributing questionnaires and talking to staff across SDL to get a more complete picture of our processing activities; and

9.4.3 reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

9.5 We document our processing activities in electronic form so we can add, remove and amend information easily.

10 Privacy notice

10.1 SDL will issue privacy notices from time to time, including 'just in time notices', informing individuals about the personal information that we collect relating to them, how they can expect their personal information to be used and for what purposes.

10.2 We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

10.3 Generally, SDL may collect information from you such as your name, contact details, contact preferences, and details of correspondence or enquiries.

10.4 If you are a customer or tenant of SDL, we may store more extensive information about you, such as arrears information, payment information, details of complaints, information on vulnerabilities and reasonable adjustments, legal documents such as tenancy agreements, outcomes of legal checks such as anti-money laundering checks, transactional information, and information about your property.

10.5 Your data will only be shared if you have agreed to it being shared or if it is necessary to share it in order to achieve a legitimate interest or it is a legal requirement that we share your data. Whether your data will be routinely shared will be notified to you in the relevant 'just in time' privacy notice. If you have any questions about who your data may be or has been shared with you can contact compliance@sdlgroup.co.uk. We do not sell any of the personal data we hold. Examples of when we may share your personal data include:

- To provide the services to you that you have requested;
- To let you know about directly relevant services provided within the Group which may be of interest to you;
- To achieve legitimate outcomes such as debt collection;
- Where we share your data to comply with a legal obligation, such as the obligation to undertake anti-money laundering checks;
- If we are legally required to share your data with law enforcement agencies.

10.6 On our websites, we use **Google Analytics**. This is a tracking cookie which enables us to track how popular a site is and to record visitor trends over time. The cookie does not contain any personal data but it does contact your computer's IP address to determine where in the world you are accessing the website from and to track your page visits within the site. We will only store this data for 38 months, in accordance with the Google Analytics retention period function. Any statistics stored for more than three years will not include any IP addresses and will not be able to identify individuals in any way.

10.7 We use **Hotjar** on our websites to create heat maps and record visits to the site and recreate them to enable us to learn more about user journeys and how visitors are really using the website.

10.7.1. The data is all anonymous and the only device-specific data we collect is:

- device's IP address (captured and stored in an anonymized format);
- device screen resolution;
- device type (unique device identifiers), operating system, and browser type;
- geographic location (country only);
- preferred language used to display the Hotjar Enabled Site.

11 Individual rights

11.1 Individuals have the following rights in relation to their personal information:

11.1.1 to be informed about how, why and on what basis that information is processed;

11.1.2 to obtain confirmation that their information is being processed and to obtain access to it and certain other information, by making a subject access request;

11.1.3 to have data corrected if it is inaccurate or incomplete;

11.1.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

11.1.5 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where SDL no longer needs the personal information but they require the data to establish, exercise or defend a legal claim; and

11.1.6 to restrict the processing of personal information temporarily where they do not think it is accurate (and SDL is verifying whether it is accurate), or where they have objected to the processing (and SDL is considering whether the organisation's legitimate grounds override their interests).

11.2 SDL trains all staff on how to respond to requests to exercise the above rights and has processes in place to ensure such requests are dealt with. If SDL is not the data controller of the data to which the right relates SDL will usually contact the data controller regarding the request before responding (depending upon the requirements set out in the contractual arrangement between SDL and the controller).

11.3 If you wish to exercise any of the above rights please contact your usual SDL point of contact, or compliance@sdlgroup.co.uk.

12 Employee obligations

12.1 SDL expects its employees to help meet its data protection obligations to individuals.

12.2 If employees have access to personal information, they must:

12.2.1 only access the personal information that they have authority to access, and only for authorised purposes;

12.2.2 only allow other SDL staff to access personal information if they have appropriate authorisation;

12.2.3 only allow individuals who are not SDL staff to access personal information if they have specific authority to do so from the Compliance Team;

12.2.4 keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in SDL's Data Protection Breach Policy);

12.2.5 not remove personal information, or devices containing personal information (or which can be used to access it), from SDL's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and

12.2.6 not store personal information on personal devices that are used for work purposes.

12.3 Staff are trained to contact the Compliance Team if they are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

12.3.1 processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in paragraph 6.1.2 being met;

12.3.2 any data breach as set out in paragraph 15.1 below;

12.3.3 access to personal information without the proper authorisation;

12.3.4 personal information not kept or deleted securely;

12.3.5 removal of personal information, or devices containing personal information (or which can be used to access it), from SDL's premises without appropriate security measures being in place;

12.3.6 any other breach of this policy or of any of the data protection principles set out in paragraph 4.1 above.

12.4 In the event of such a report, SDL will fully investigate and rectify the situation.

13 Information security

13.1 SDL will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

13.1.1 making sure that, where possible, personal information is encrypted;

13.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

13.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and

13.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

13.2 Where SDL uses external organisations to process personal information on its behalf, additional security arrangements will be implemented in contracts with those organisations

to safeguard the security of personal information. In particular, contracts with external organisations provide that:

13.2.1 the organisation may act only on the written instructions of SDL;

13.2.2 those processing the data are subject to a duty of confidence;

13.2.3 appropriate measures are taken to ensure the security of processing;

13.2.4 sub-contractors are only engaged with the prior consent of SDL and under a written contract;

13.2.5 the organisation will assist SDL in providing subject access and allowing individuals to exercise their rights in relation to data protection;

13.2.6 the organisation will assist SDL in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;

13.2.7 the organisation will delete or return all personal information to SDL as requested at the end of the contract unless legally required to keep the data; and

13.2.8 the organisation will submit to audits and inspections, provide SDL with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell SDL immediately if it is asked to do something infringing data protection law.

13.3 Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the Compliance Team.

14 Storage and retention of personal information

14.1 Personal information (and sensitive personal information) will be kept securely in accordance with SDL's Information Security and Data Protection Breach Policy.

14.2 Personal information (and sensitive personal information) will not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff follow SDL's Record Management Policy which sets out the relevant retention period, or the criteria that should be used to determine the retention period.

14.3 Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

15 Data breaches

15.1 A data breach may take many different forms, for example:

15.1.1 loss or theft of data or equipment on which personal information is stored;

15.1.2 unauthorised access to or use of personal information either by a member of staff or third party;

15.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

15.1.4 human error, such as accidental deletion or alteration of data;

15.1.5 unforeseen circumstances, such as a fire or flood;

15.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

15.1.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

15.2 SDL will:

15.2.1 make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

15.2.2 notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law

unless SDL is not the Data Controller, in which case SDL shall report the breach as soon as possible to the relevant Data Controller.

16 International transfers

16.1 SDL will not transfer personal information outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway unless appropriate safeguards are in place.

17 Training

17.1. SDL will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

17.2. SDL keep a log of all employee data protection training and testing to ensure that all staff have competent knowledge of data protection requirements.

18 Consequences of employees failing to comply

18.1 SDL takes compliance with this policy very seriously. Failure to comply may result in disciplinary action against our employees, including dismissal. Employees are informed about the importance of maintaining data protection compliance at all times and are informed that if they fail to do so they could be subject to disciplinary action, including dismissal.

18.2 If you have any questions or concerns about anything in this policy, do not hesitate to contact the Compliance Team at compliance@sdlgroup.co.uk.