Data Protection Policy

- **Introduction**

Surecall is committed to all aspects of data protection and takes seriously its duties, and the duties of its colleagues, under the Data Protection Act 1998. This policy sets out how SC deals with personal data, including personnel files and data subject access requests, and colleagues' obligations in relation to personal data.

- **Data protection principles**

The Data Protection Act 1998 requires that eight data protection principles be followed in the handling of personal data. These principles require that personal data must:

- be fairly and lawfully processed
- be processed for limited purposes and not in any manner incompatible with those purposes
- be adequate, relevant, and not excessive
- be accurate
- not be kept longer than is necessary
- be processed in accordance with individuals' rights
- be secure; and not be transferred to countries without adequate protection.

- **Personal data**

The Data Protection Act 1998 applies only to information that constitutes "personal data". Information is "personal data" if it:

- identifies a person, whether by itself, or together with other information in the organisation's possession, or is likely to come into its possession; and
- is about a living person and affects that person's privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature.
- Consequently, automated and computerised personal information about colleagues held by employers is covered by the Act. Personal information stored physically (for example, on paper) and held in any "relevant filing system" is also covered. In addition, information recorded with the intention that it will be stored in a relevant filing system or held on computer is covered.
- A "relevant filing system" means a well-structured manual system that amounts to more than a bundle of documents about each colleagues filed in date order, i.e. a system to guide a searcher to where specific information about a named colleagues can be located easily.

4. The use of personal information

The Data Protection Act 1998 applies to personal information that is "processed". This includes obtaining personal information, retaining, and using it, allowing it to be accessed, disclosing it and, finally, disposing of it.

5. Sensitive personal data

- Sensitive personal data" is information about a colleague's:
- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- physical or mental health or condition
- sex life
- commission or alleged commission of any criminal offence; and proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

Surecall will not retain sensitive personal data without the express consent of the colleagues in question.

Surecall will process sensitive personal data, including sickness and injury records and references, in accordance with the eight data protection principles. If Surecall enters into discussions about a merger or acquisition with a third party, Surecall will seek to protect colleagues' data in accordance with the data protection principles.

6. Personnel files

- A colleagues personnel file is likely to contain information about his/her work history with Surecall and may, for example, include information about any disciplinary or grievance procedures, warnings, absence records, appraisal or performance information and personal information about the colleague including address details and national insurance number.
- There may also be other information about the colleagues located within Surecall, for example in his/her line manager's inbox or desktop; with payroll; or within documents stored in a relevant filing system.
- Surecall may collect relevant sensitive personal information from colleagues for equal opportunities monitoring purposes. Where such information is collected, Surecall will anonymise it unless the purpose to which the information is put requires the full use of the individual's personal information. If the information is to be used, Surecall will inform colleagues on any monitoring questionnaire of the use to which the data will be put, the individuals or posts within Surecall who will have access to that information and the security measures that Surecall will put in place to ensure that there is no unauthorised access to it.

- Surecall will ensure that personal information about a colleague, including information in personnel files, is securely retained. SC will keep hard copies of information in a locked filing cabinet. Information stored electronically will be subject to access controls and passwords and encryption software will be used where necessary.
- Where laptops are taken off site, colleagues must follow SC relevant policies relating to the security of information and the use of computers for working at home/bringing your own device to work.

7. **Data subject access requests**

The organisation will inform each colleague of:

- the types of information that it keeps about him/her
- the purpose for which it is used and
- the types of organisation that it may be passed to, unless this is self-evident (for example, it may be self-evident that an colleagues' national insurance number is given to HM Revenue & Customs).
- A colleague has the right to access information kept about him/her by Surecall, including personnel files, sickness records, disciplinary or training records, appraisal or performance review notes, emails in which the colleagues is the focus of the email and documents that are about the colleagues.
- Surecall may charge up to £10 for allowing colleagues access to information about them. Surecall will respond to any data subject access request within 40 calendar days.
- Surecall will allow the colleagues access to hard copies of any personal information. However, if this involves a disproportionate effort on the part of Surecall the colleagues shall be invited to view the information on-screen or inspect the original documentation at a place and time to be agreed by Surecall.
- Surecall may reserve its right to withhold the colleagues' right to access data where any statutory exemptions apply.

8. Correction, updating and deletion of data

The organisation has a system in place that enables colleagues to check their personal information on a regular basis so that they can correct, delete, or update any data. If a colleague becomes aware that SC holds any inaccurate, irrelevant, or out-of-date information about him/her, he/she must notify the People Team immediately and provide any necessary corrections and/or updates to the information.

9. Data that is likely to cause substantial damage or distress

If a colleague believes that the processing of personal information about him/her is causing, or is likely to cause, substantial and unwarranted damage or distress to him/her or another person. He/she should notify the People team in writing to request that Surecall put a stop to the processing of that information. Within 21 days of receiving the colleagues' notice, Surecall will reply to the colleague stating either: that it has complied with or intends to comply with the request; or the

reasons why it regards the colleagues' notice as unjustified to any extent and the extent, if any, to which it has already complied or intends to comply with the notice.

10. Monitoring

Surecall may monitor colleagues by various means including, but not limited to, recording colleagues' activities on CCTV, checking emails, listening to voicemails, and monitoring telephone conversations. If this is the case, Surecall will inform the colleagues that monitoring is taking place, how the data is being collected, how the data will be securely processed and the purpose for which the data will be used. Colleagues will usually be entitled to be given any data that has been collected about him/her. Surecall will not retain such data for any longer than is necessary.

In exceptional circumstances, Surecall may use monitoring covertly. This may be appropriate where there is, or could potentially be, damage caused to Surecall by the activity being monitored and where the information cannot be obtained effectively by any non-intrusive means (for example, where an colleagues is suspected of stealing property belonging to Surecall. Covert monitoring will take place only with the approval of the People Team.

11. Colleagues obligations regarding personal information

- If a colleague acquires any personal information in the course of his/her duties, he/she must ensure that:
- the information is accurate and up to date, insofar as it is practicable to do so
- the use of the information is necessary for a relevant purpose and that it is not kept longer than necessary; and the information is secure.

Colleagues should ensure that he/she:

- uses password-protected and encrypted software for the transmission and receipt of emails
- sends fax transmissions to a direct fax where possible and with a secure cover sheet and locks files in a secure cabinet
- Where information is disposed of, colleagues should ensure that it is destroyed. This may involve the permanent removal of the information from the server, so that it does not remain in a colleagues' inbox or trash folder. Hard copies of information may need to be confidentially shredded. Colleagues should be careful to ensure that information is not disposed of in a wastepaper basket/recycle bin.
- If a colleague acquires any personal information in error by whatever means, he/she shall inform the People team immediately and, if it is not necessary for him/her to retain that information, arrange for it to be handled by the appropriate individual within Surecall.
- Where a colleague is required to disclose personal data to any other country, he/she must ensure first that there are adequate safeguards for the protection of data in the host country. For further guidance on the transfer of personal data outside the UK, please contact the People team.
- A colleague must not take any personal information away from Surecall premises, save in circumstances where he/she has obtained the prior consent of the People team or Senior Management to do so.

- If a colleague is in any doubt about what he/she may or may not do with personal information, he/she should seek advice from the People team. If he/she cannot get in touch with them, he/she should not disclose the information concerned.

12. Consequences of non-compliance

- All colleagues are under an obligation to ensure that they have regard to the eight data protection principles (see above) when accessing, using, or disposing of personal information. Failure to observe the data protection principles within this policy may result in a colleague incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal. For example, if a colleague accesses another colleagues' employment records without the requisite authority, Surecall will treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.

13. Taking employment records off site

- Colleagues must not take employment records off site (whether in electronic or paper format) without prior authorisation from the People team or Senior Management.
- Colleagues may take only certain employment records off site. These are documents relating to disciplinary or grievance meetings that cannot be held on site/meetings with occupational health/discussions surrounding the sale of the business or specific monitoring purposes/seeking professional advice. Colleagues may also take employment records off site for any other valid reason given by the People team or Senior Management.
- Any colleagues taking records off site must ensure that he/she does not leave his/her laptop, other device, or any hard copies of employment records on the train, in the car or any other public place. He/she must also take care when observing the information in hard copy or on-screen that such information is not viewed by anyone who is not legitimately privy to that information.

14. Review of procedures and training

- Surecall will provide training to all colleagues on data protection matters on induction and on a regular basis thereafter. If any colleagues consider that he/she would benefit from refresher training, he/she should contact the People team.
- Surecall will review and ensure compliance with this policy at regular intervals.

Tony Elia

Company Director

Surecall Recruitment Ltd

August 2020