Privacy Notice – SCC Employees / Contractors

Your privacy is important to us. This Privacy Notice explains what personal data we collect from you (as a current or former Employee or Contractor of SCC) and how we use it.

If you are NOT a current or former SCC Employee, then please refer to SCC's public Privacy Notice which can be found here.

Important Information: Specialist Computer Centres plc ("SCC") is a company registered in England under company number 01428210. Our registered office is James House, Warwick Road, Birmingham B11 2LE. For the purposes of data protection laws, we will be the data controller for certain personal data collected from you in the circumstances described below, and our Data Protection Officer can be contacted atDPO@scc.com, or on 0121 766 7000.

What information we collect

SCC collects data to operate effectively and we are committed to protecting the privacy and security of your personal information. We are a data controller over this data and as such we are responsible for deciding how we process it. The purpose of this Privacy Notice is to explain those decisions.

The type and amount of data we collect varies according to your relationship with us, but as an Employee or a Contractor, it is likely to include some or all of the items below:

- **Name and contact data**. We collect your first and last name, email address, postal address, phone number and other similar contact data.
- **Additional personal data**. We collect additional personal and identification information (including your photograph), date of birth and gender, marital status, next of kin, dependants and emergency contacts.
- **Financial data**. We collect salary, benefit and tax data, details of your bank account and National Insurance number.
- **Employment data**. We collect terms and conditions of your employment (including nationality, entitlement to work, CV and references), performance, qualifications and employment history.
- **HR data**. We collect details of any absences, leave, disciplinary proceedings or grievance proceedings.
- **Driver data**. We collect driver and vehicle data

- **Security data**. We collect security clearance data and data which may be required for site access, including photo ID in some cases
- **Correspondence**. We collect the content of messages, e-mails, letters or phone calls you send us. As part of this, certain phone conversations may be monitored and recorded.
- **CCTV**. If you enter SCC buildings, your image may be captured by our security cameras. We will regularly delete CCTV footage, unless it is being used to investigate an alleged crime or an incident, in which case it may be retained for up to 1 year following the conclusion of any investigation.
- We may collect other relevant information required to ensure SCC fulfil our obligations as an employer.

In addition, we may collect and process certain types of Special Category personal data where this is absolutely required. This includes:

- **Health data**. Information about medical or health conditions for which the organisation needs to make reasonable adjustments or as a result of health and safety assessments conducted in relation to your role. This type of data may also be collected and used in sickness absence management.

We collect this personal information initially through the application and recruitment process, either directly from you or perhaps through an employment agency, and then collect additional information through the course of job-related activities whilst you are employed by SCC.

We may also carry out checks with CIFAS for any fraudulent activity or history. You can find out how CIFAS handles your personal data in Appendix 1 below.

Why we process your information

Primarily, we collect and process your personal data to **fulfil your contract of employment**. This includes ensuring we comply with legal requirements such as paying tax and National Insurance, checking your right to work in the UK and making reasonable adjustments for disabled employees.

There may also be circumstances where we additionally process your data on one or more of the following lawful bases:

- **Because it is in our legitimate interest.** We also sometimes process your information in pursuit of our legitimate interests to:
    - improve our business (including internal communications and engagement activities) and operate it efficiently and legally;
    - prevent fraud; and
    - ensure general safety and security.

When we process your information on that basis, we always make sure that we balance our interest in having the information with your rights and reasonable expectations.

- **Because we need it to comply with the law.** In some rare cases, we will need to retain your information because we are compelled to do so by law.

What we do with it

In relation to your personal data, we will:

- process it fairly, lawfully and in a clear, transparent way
- collect your data only for reasons that we find proper for the course of your employment in ways that have been explained to you

- only use it in the way that we have told you about
- ensure it is correct and up to date
- keep your data for only as long as we need it
- process it in a secure manner that ensures it will not be misused, lost or destroyed

If you do not provide your data to us

One of the reasons for processing your data is to allow us to carry out our duties in line with your contract of employment. If you do not provide us with the data needed to do this, we will unable to perform those duties e.g. ensuring you are paid correctly. We may also be prevented from confirming, or continuing with, your employment with us in relation to our legal obligations if you do not provide us with this information e.g. confirming your right to work in the UK or, where appropriate, confirming your legal status for carrying out your work via a criminal records check.

How we share your data

We share your personal data with colleagues within SCC as necessary for them to complete their duties. This includes, but is not limited to, your line manager for their management of you, the HR department for maintaining personnel records and the payroll department for administering payment under your contract of employment.

We may also share your personal data with other entities within the SCC Group of companies, including affiliates and subsidiaries. This is also done only as necessary for them to perform their duties. These entities may exist within the UK or within the European Economic Area (most notably SCC's wholly owned subsidiary in Romania).

In some cases, we may need to transfer your information outside of the European Economic Area because we (or a third party or vendor we use) store it on systems that are hosted abroad, or because we need to share it with companies that are not situated in the European Economic Area.

Some of our support operations in Vietnam may be able to access your data; this is primarily for the purpose of enabling the provision of internal IT support. The data is encrypted in transit and our staff in Vietnam are subject to strict security measures and will only access data where necessary. The support operations in Vietnam are also able to access content on SCC's intranet, for staff engagement and internal communications purposes. In some cases this may contain personal data.

Where we transfer your information outside the European Economic Area, we will always ensure that your information is safe and only sent to organisations providing adequate safeguards, such as:

- Organisations established in countries providing adequate provisions to safeguard your personal information;
- Organisations who are contractually bound to protect your information.

We may also transfer your data abroad if we have a legal obligation to do so.

We may also disclose personal data as part of a corporate transaction such as a merger or acquisition.

In addition, we may share your details with selected suppliers or vendors we hire to carry out certain tasks on our behalf, and to exercise or defend our legal rights and fulfil our legal obligations. Our partner companies must abide by our data privacy and security requirements, and are not allowed to use personal data they receive from us for any other purpose.

Your rights

You have rights over how SCC uses your data, and unless your request to exercise those rights is complex or there are numerous requests, we will normally respond within one month of receipt of your request.

Your rights include:

- **Access.** You have a right to know whether we hold personal information about you. Where this is the case, you can request a copy of your personal data held, as well as information about how it is being used. However, please note that your right of access is subject to limits and we may not be able to provide you with all the requested information. Where this is the case, we will explain the reasons why. Your request will be responded to within one calendar month of receipt. Please note that we may require you to provide proof of identity before we are able to provide any information.
- **Rectification.** Where information held about you is inaccurate or incomplete, you may request its rectification or completion.
- **Erasure.** In certain circumstances, you may request your information to be erased (subject to conditions).
- **Restriction.** You have a right to ask us to restrict our use of your personal information in some circumstances, for example whilst we investigate a complaint that the data we hold about you is inaccurate (subject to conditions).
- **Portability.** In certain circumstances, you may request the movement, copy or transfer of your information (subject to conditions).
- **Objection.** You have a right to object to the use of your information. Additionally, where we have used your information in pursuit of our legitimate interests, you can ask us to stop (subject to conditions).

Should you wish to exercise those rights, please contact our Data Protection Officer at DPO@scc.com.

Complaints. If you wish to raise a complaint on how we have handled your personal data, you can contact our Data Protection Officer at DPO@scc.com, who will investigate the matter. If you are dissatisfied with our response or believe we are not processing your personal data in accordance with the law, you can complain to the Information Commissioner's Office (www.ico.org.uk).

How long we keep your information

SCC retains your personal data only for as long as necessary to fulfil our purposes for processing it. Generally, this will be for at least the duration of your employment with us.

Beyond that, in some cases, we will continue to retain your data beyond your period of employment. The duration of this retention will vary depending on the circumstances but will always be underpinned by a legitimate need to retain the data (such as adherence to statutory retention requirements) and will be done in compliance with SCC's published Information Retention Policy.

The criteria below are good indicators of how we decide how long to keep data for:

- How long is the personal data needed to effectively operate our business? This includes such things as maintaining good business and financial records. This is the general rule that establishes the baseline for most data retention periods.

- Is SCC subject to a legal, contractual or similar obligation to retain the data? This includes cases where the law prescribes we should keep information for a given period of time, or where data must be preserved during an investigation, for current or potential litigation or contractual purposes. Some data must also be kept for audit purposes.
- Whether the data protection authority has provided guidance or recommendations for specific data or document types.

Security of your information

We apply technical and organisational security measures to protect your information and protect it from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure. The security measures we apply vary depending on the type of data at stake, the reasons why we hold it and any specific risks.

The effectiveness of our security controls are assessed and verified periodically as part of our certification to ISO 27001, the International Standard for Information Security management, which applies to our whole business. We require all our staff and any third parties who carry out work on our behalf to comply with our security policies and appropriate compliance standards.

Links to other websites

This privacy notice does not cover the links within this site linking to other websites. We encourage you to read the privacy statements on the other websites you visit.

Changes to this Privacy Notice

This Policy (ref: SCC-NOT-00503 – v5.0) was last updated on 31st March 2023. If we change our Privacy Notice or Cookies Policy, we will update the changes on this website. We may also place notices on other pages of the website so you may check our current policy at any time.

Appendix 1 CIFAS Fair Processing Notice

GENERAL

1. We will check your details against the Cifas databases established for the purpose of allowing organisations to record and share data on their fraud cases, other unlawful or dishonest conduct, malpractice, and other seriously improper conduct ("Relevant Conduct") carried out by their staff and potential staff. "Staff" means an individual engaged as an employee, director, trainee, homeworker, consultant, contractor, temporary or agency worker, or self-employed individual, whether full or part time or for a fixed-term.
2. The personal data you have provided, we have collected from you, or we have received from third parties will be used to prevent fraud and other relevant conduct and to verify your identity.
3. Details of the personal information that will be processed include: name, address, date of birth, any maiden or previous name, contact details, document references, National Insurance Number, and nationality. Where relevant, other data including employment details will also be processed.
4. We and Cifas may also enable law enforcement agencies to access and use your personal data to detect, investigate, and prevent crime.
5. We process your personal data on the basis that we have a legitimate interest in preventing fraud and other Relevant Conduct, and to verify identity, in order to protect our business and customers and to comply with laws that apply to us. This processing of your personal data is also a requirement of your engagement with us.
6. Cifas will hold your personal data for up to six years if you are considered to pose a fraud or Relevant Conduct risk.

CONSEQUENCES OF PROCESSING

1. Should our investigations identify fraud or any other Relevant Conduct by you when applying for or during the course of your engagement with us, your new engagement may be refused or your existing engagement may be terminated or other disciplinary action taken (subject to your rights under your existing contract and under employment law generally).
2. Fraud prevention databases have been established for the purpose of allowing employers to share data on their employment fraud cases.
   Should our investigations identify fraud or the commission of any other criminal offence by you [on your part] when applying for, or during the course of your employment with us, we will record the details of this on the relevant fraud prevention databases. This information may be accessed from the UK and other countries and used by law enforcement agencies and by us and other organisations to prevent fraud.
   Please contact us at HR@scc.com if you want to receive details of the relevant fraud prevention databases through which we share information.

DATA TRANSFERS

1. A record of any fraudulent or other Relevant Conduct by you will be retained by Cifas and may result in others refusing to employ you. If you have any questions about this, please contact us using the details provided.
2. Should Cifas decide to transfer your personal data outside of the European Economic Area, they will impose contractual obligations on the recipients of that data to protect your personal data to the standard required in the European Economic Area. They may also require the recipient to subscribe to 'international frameworks' intended to enable secure data sharing.

YOUR RIGHTS

1. Your personal data is protected by legal rights, which include your rights to object to our processing of your personal data, request that your personal data is erased or corrected, and request access to your personal data.
2. For more information or to exercise your data protection rights please, please contact us using the contact details provided.
3. You also have a right to complain to the Information Commissioner's Office which regulates the processing of personal data.