Privacy Notice – SCC Careers

Your privacy is important to us. This Privacy Notice explains what personal data we collect from you and how we use it.

If you are a current or former SCC Employee, then please refer to the SCC Employee 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 at Protect@scc.com, or on 0121 766 7000.

What information we collect

We collect information about you in order to assess your suitability for a job you have applied for / we have contacted you about. We ensure that we only collect the minimum amount of information necessary to process your application and you may decline to disclose some personal data. However, we may be unable to process your application if the data you decline to provide is necessary for SCC to be able to assess your suitability for the role.

- **Name and contact data.** We collect your first and last name, email address, phone number and other similar contact data.
- **Location.** We collect information about the area where you reside to help us match your profile with openings we have in specific geographical areas.
- **Work and education history.** We collect information about any qualifications, certifications, degrees you may have obtained, as well as about your previous work experience, such as reasons for leaving a previous employer.
- **Financial information.** We may collect information on your current salary or package, and your salary expectations.
- **Your interactions with us.** We may collect the content of messages, e-mails, or letters you send us, as well as questions and information you ask us.
- **Assessments.** As part of the recruitment process, we may ask you to take personality questionnaires, or to complete tests. In some cases, we may formalise feedback on your overall performance.
- **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

- **Referees.** We collect information about individuals you list as referees, such as their name, work address, job title and the company they work for.
- **Identification, fraud checks and security clearances.** If you are invited to an interview, we will request sight of your right to work documentation.

Depending on the type of role you apply for, we may also require details of your security clearance status and you may be asked to go through the security clearance process if required. We will inform you of how your information will be handled at the relevant time.

We will 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.

How we collect your information

You provide some of the personal data we hold about you directly when submitting your application or interacting with our recruitment team, for example via the SCC Careers webpage, via email, or over the phone.

We also get some information about you from third parties such as LinkedIn, JobServe, CV Library and other recruitment agencies when you respond to an ad placed on those websites.

We get some of it by recording how you interact with our products by, for example, using technologies like cookies. For more information on this, please see our Cookies policy here.

Why we process your information

There are multiple legal grounds on which we may process your information.

- **Because you have agreed.** Where possible, we collect information about you with your consent. This is the case, for instance, when you fill in paper or online forms and choose to provide us with your information. You may withdraw your consent at any time by emailing Protect@scc.com.
- **Because it is in our legitimate interest.** We also sometimes process your information in pursuit of our legitimate interests to:
    - attract, onboard and retain talent;
    - improve our business and operate it efficiently;
    - 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. This will be the case for instance when we check you have a right to work in the United Kingdom.

What we do with your information

We process personal data about you in order to assess your suitability for a job you have applied for or we have contacted you about. All of the information you provide during the process will only be

used for the purpose of progressing your application, to keep you updated of other opportunities you may be interested in, or to fulfil legal or regulatory requirements where necessary.

How we share your data

Your personal data is not routinely shared with any third party. In the unlikely event that we would need, in future, to share your information in specific circumstances, we will ensure that this is done in accordance with the law.

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 solely 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.

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;
- Organisations who have obtained Privacy Shield certification.

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

Your rights

You have rights over how SCC use your data, and unless your request to exercise those rights is we will normally respond within one month of receipt of your request.

- **Access.** You have a right to know whether we hold personal information about you. Where such 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 Protect@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 Protect@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

If you are successful and become an employee, the information you provide during the application process will be retained by us as part of your employee file for the duration of your employment and then in line with our published information retention policy following the end of your employment. This includes your criminal records declaration, fitness to work, records of any security checks and references.

In any other case, the information you have provided may be retained for up to 12 months. Any information generated throughout the assessment/interview process will be retained by us for 3 months following the closure of the campaign.

SCC only retains personal data for as long as necessary to provide you with the services you have requested, to operate our business, or for other essential purposes such as complying with our legal obligations, resolving disputes and enforcing our agreements. We will keep your data in line with our Information Retention Policy, and retention periods will vary for different types of data.

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

- How long is the personal data needed to provide the services and 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.
- Have you provided consent for a longer retention period? If so, we will retain data in accordance with your consent.

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-00508 – v4.0) was last updated on 14th April 2020. 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 you 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.