

	SCS Building Solutions Ltd	Section:	Policy Document
	Policy Document	Reference:	PD 009
	GDPR Policy	Page No:	Page 1 of 8

GDPR Policy

Policy Statement

SCS Building Solutions Ltd (SCS) takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the Data Protection Act 2018 and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

This policy applies to current and former employees, workers, volunteers, apprentices, and consultants. If you fall into one of these categories then you are a 'Data Subject' for the purposes of this policy. You should read this policy alongside your Contract of Employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

SCS has measures in place to protect the security of your data in accordance with this policy. SCS will only hold data for as long as necessary for the purposes for which it was collected, or in accordance with any retention period prescribed by Law. SCS is a 'Data Controller' for the purposes of your 'Personal Data'. This means that we determine the purpose and means of the processing of your 'Personal Data'.

This policy explains how SCS will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing, or storing 'Personal Data' in the course of working for, or on behalf of, SCS.

This policy does not form part of your Contract of Employment (or contract for services if relevant) and can be amended by SCS at any time. It is intended that this policy is fully compliant with the Data Protection Act 2018 and GDPR. If any conflict arises between those laws and this policy, SCS intends to comply with the Data Protection Act 2018 and the GDPR.

Data Protection Principles

'Personal Data' must be processed in accordance with seven 'Data Protection Principles.' These are: -

- It must be processed fairly, lawfully, and transparently.
- It must be collected and processed only for specified, explicit and legitimate purposes.
- It must be adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
- It must be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay.
- It must not be kept for longer than is necessary for the purposes for which it is processed; and
- It must be processed securely.
- SCS are accountable for the proper processing of personal data and compliance with the rules of the GDPR.

Signed:



Name: Paul Flynn

Date: 24/10/2023

Issue:	4	Issue Date:	October 2023	Review Date:	October 2024	Authorised By:	Paul Flynn
--------	---	-------------	--------------	--------------	--------------	----------------	------------

Contents

Section 1 - How We Define ‘Personal Data’	2
Section 2 - How We Define Special Categories of ‘Personal Data’	3
Section 3 - How We Define ‘Processing’	3
Section 4 - How Will We Process your ‘Personal Data’	3
Section 5 - Examples of When We Might Process your ‘Personal Data’	4
Section 6 - Sharing your ‘Personal Data’	5
Section 7 - How Should You Process Personal Data for SCS	6
Section 8 - How to Deal with Data Breaches	6
Section 9 - Subject Access Requests	7
Section 10 - Your Data Subject Rights	7
Section 11 – Data Retention Policy	8
Distribution	8

Section 1 - How We Define ‘Personal Data’

‘Personal Data’ - Information which relates to a living person (a ‘data subject’) who can be identified from that on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all ‘Personal Data’ whether it is stored electronically, on paper or on other materials.

This ‘Personal Data’ might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the Contract of Employment (or services) or after its termination. It could be created by your Manager or other colleagues. We will collect and use the following types of ‘Personal Data’ about you: -

- Recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments.
- Your contact details and date of birth.
- The contact details for your emergency contacts.
- Your gender.
- Your marital status and family details.
- Information about your Contract of Employment (or services) including start and end dates of employment, role, and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits, and holiday entitlement.
- Your bank details and information in relation to your tax status including your national insurance number.
- Your identification documents including passport and driving license and information in relation to your immigration status and right to work for us.

	SCS Building Solutions Ltd	Section:	Policy Document
	Policy Document	Reference:	PD 009
	GDPR Policy	Page No:	Page 3 of 8

- Information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings).
- Information relating to your performance and behaviour at work.
- Training records.
- Electronic information in relation to your use of IT systems/swipe cards/telephone systems.
- Your images (whether captured on CCTV, by photograph or video).
- iTunes passwords and computer passwords.
- Any other category of 'Personal Data' which we may notify you of from time to time.

Section 2 - How We Define Special Categories of 'Personal Data'

'Special categories of Personal Data' are types of 'Personal Data' consisting of information as to: -

- Your racial or ethnic origin.
- Your political opinions.
- Your religious or philosophical beliefs.
- Your trade union membership.
- Your genetic or biometric data.
- Your health.
- Your sex life and sexual orientation; and
- Any criminal convictions and offences.

We may hold and use any of these special categories of your 'Personal Data' in accordance with the law.

Section 3 - How We Define 'Processing'

'Processing' means any operation which is performed on 'Personal Data' such as: -

- Collection, recording, organisation, structuring or storage.
- Adaption or alteration.
- Retrieval, consultation, or use.
- Disclosure by transmission, dissemination or otherwise making available.
- Alignment or combination; and
- Restriction, destruction, or erasure.

This includes processing 'Personal Data' which forms part of a filing system and any automated processing.

Section 4 - How Will We Process your 'Personal Data'

SCS will process your 'Personal Data' (including special categories of Personal Data) in accordance with our obligations under the 2018 Act.

We will use your 'Personal Data' for: -

- Performing the Contract of Employment (or services) between us.

Issue:	4	Issue Date:	October 2023	Review Date:	October 2024	Authorised By:	Paul Flynn
--------	---	-------------	--------------	--------------	--------------	----------------	------------

	SCS Building Solutions Ltd	Section:	Policy Document
	Policy Document	Reference:	PD 009
	GDPR Policy	Page No:	Page 4 of 8

- Complying with any legal obligation; or
- If it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in section 10 below.

We can process your ‘Personal Data’ for these purposes without your knowledge or consent. We will not use your ‘Personal Data’ for an unrelated purpose without telling you about it and the Legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain ‘Personal Data’ you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

Section 5 - Examples of When We Might Process your ‘Personal Data’

We have to process your ‘Personal Data’ in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

For example: -

- To decide whether to employ (or engage) you.
- To decide how much to pay you, and the other terms of your contract with us.
- To check you have the legal right to work for us.
- To carry out the contract between us including where relevant, its termination.
- Training you and reviewing your performance*.
- To decide whether to promote you.
- To decide whether and how to manage your performance, absence, or conduct*.
- To carry out a disciplinary or grievance investigation or procedure in relation to you or someone else.
- To determine whether we need to make reasonable adjustments to your workplace or role because of your disability*.
- To monitor diversity and equal opportunities*.
- To monitor and protect the security (including network security) of SCS, of you, our other staff, customers, and others.
- To monitor and protect the health and safety of SCS, of you, our other staff, customers and third parties*.
- To pay you and provide pension and other benefits in accordance with the contract between us*.
- Paying tax and national insurance.
- To provide a reference upon request from another employer.
- To pay trade union subscriptions*.

Issue:	4	Issue Date:	October 2023	Review Date:	October 2024	Authorised By:	Paul Flynn
--------	---	-------------	--------------	--------------	--------------	----------------	------------

	SCS Building Solutions Ltd	Section:	Policy Document
	Policy Document	Reference:	PD 009
	GDPR Policy	Page No:	Page 5 of 8

- Monitoring compliance by you, us and others with our policies and our contractual obligations*.
- To comply with Employment Law, Immigration Law, Health and Safety Law, Tax Law and other laws which affect us*.
- To answer questions from insurers in respect of any insurance policies which relate to you*.
- Running our business and planning for the future.
- The prevention and detection of fraud or other criminal offences.
- To defend SCS in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*.
- For any other reason which we may notify you of from time to time.

*We might process special categories of your 'Personal Data' for the purposes above which have an asterisk beside them. In particular, we may use information in relation to; your sickness absence, health, and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under Employment Law including to make reasonable adjustments and to look after your health and safety.

We will only process special categories of your 'Personal Data' (see above) in certain situations in accordance with the Law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of 'Personal Data' then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting Craig Scott.

We do not need your consent to process special categories of your 'Personal Data' when we are processing it for the following purposes, which we may do: -

- Where it is necessary for carrying out rights and obligations under Employment Law.
- Where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent.
- Where you have made the data public.
- Where processing is necessary for the establishment, exercise, or defence of Legal claims; and
- Where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

We do not take automated decisions about you using your 'Personal Data' or use profiling in relation to you.

Section 6 - Sharing your 'Personal Data'

Sometimes we might share your 'Personal Data' with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

We require those companies to keep your 'Personal Data' confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

We require Azets to keep your 'Personal Data' confidential and secure to enable them to complete the payroll.

We require Perspective (HNN) Ltd, Aviva and Now Pensions to keep your 'Personal Data' confidential and secure to enable them to administer the SCS Pension Scheme.

SCS requires 'Personal Data' to be held on E-days in order to track absences and annual leave.

Issue:	4	Issue Date:	October 2023	Review Date:	October 2024	Authorised By:	Paul Flynn
--------	---	-------------	--------------	--------------	--------------	----------------	------------

	SCS Building Solutions Ltd	Section:	Policy Document
	Policy Document	Reference:	PD 009
	GDPR Policy	Page No:	Page 6 of 8

We do not send your 'Personal Data' outside the European Economic Area (EEA). If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

Section 7 - How Should You Process Personal Data for SCS

Everyone who works for, or on behalf of, SCS has some responsibility for ensuring data is collected, stored, and handled appropriately, in line with this policy. SCS's Data Protection Officer/Data Protection Manager Craig Scott is responsible for reviewing this policy and updating the Board of Directors on SCS's data protection responsibilities and any risks in relation to the processing of data.

You should: -

- Direct any questions in relation to this policy or data protection to the Data Protection Manager.
- Only access 'Personal Data' covered by this Policy if you need it for the work you do for, or on behalf of SCS and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.
- Keep 'Personal Data' secure and not share it with unauthorised people.
- Regularly review and update 'Personal Data' which you have to deal with for work. This includes telling us if your own contact details change.
- Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.
- Lock drawers and filing cabinets, do not leave paper with 'Personal Data' lying about. Consider a clear desk policy.
- Shred and dispose of 'Personal Data' securely when you have finished with it.
- Ask for help from your Line Manager or our Data Protection Officer if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

You should not: -

- Share 'Personal Data' informally.
- Make unnecessary copies of 'Personal Data' and should keep and dispose of any copies securely.
- Save 'Personal Data' to your own personal computers or other devices.
- Take 'Personal Data' away from company's premises without authorisation from your Line Manager.

Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our Disciplinary Procedure.

'Personal Data' should never be transferred outside the European Economic Area except in compliance with the Law and authorisation of the Data Protection Officer.

It is a criminal offence to conceal or destroy 'Personal Data' which is part of a subject access request (see below section 8). This conduct would also amount to gross misconduct under our Disciplinary Procedure, which could result in your dismissal.

Section 8 - How to Deal with Data Breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of 'Personal Data' occur (whether in respect of you or someone else) then we must take

Issue:	4	Issue Date:	October 2023	Review Date:	October 2024	Authorised By:	Paul Flynn
--------	---	-------------	--------------	--------------	--------------	----------------	------------

	SCS Building Solutions Ltd	Section:	Policy Document
	Policy Document	Reference:	PD 009
	GDPR Policy	Page No:	Page 7 of 8

notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner’s Office within 72 hours.

If you are aware of a data breach you must contact Craig Scott immediately and keep any evidence you have in relation to the breach.

Section 9 - Subject Access Requests

Data subjects can make a ‘subject access request’ (‘SAR’) to find out the information we hold about them. This request must be made in writing. If you receive such a request, you should forward it immediately to Craig Scott the Data Protection Officer who will coordinate a response.

If you would like to make a SAR in relation to your own ‘Personal Data’ you should make this in writing to Craig Scott. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months. There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive, we may charge a reasonable administrative fee or refuse to respond to your request.

Section 10 - Your Data Subject Rights

You have the right to information about what ‘Personal Data’ we process, how and on what basis as set out in this policy.

You have the right to access your own ‘Personal Data’ by way of a subject access request (see above). You can correct any inaccuracies in your ‘Personal Data’, to do so you should contact Craig Scott. While you are requesting that your ‘Personal Data’ is corrected or erased or are contesting the Lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact Craig Scott.

You have the right to request that we erase your ‘Personal Data’ where we were not entitled under the law to process it, or it is no longer necessary to process it for the purpose it was collected. To do so you should contact Craig Scott.

You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

You have the right to object if we process your ‘Personal Data’ for the purposes of direct marketing.

You have the right to receive a copy of your ‘Personal Data’ and to transfer your ‘Personal Data’ to another data controller. We will not charge for this and will in most cases aim to do this within one month.

With some exceptions, you have the right not to be subjected to automated decision-making.

You have the right to be notified of a data security breach concerning your ‘Personal Data’.

In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your ‘Personal Data’ for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact Craig Scott.

You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner’s Office directly. Full contact details including a helpline number can be found on the Information Commissioner’s Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

Issue:	4	Issue Date:	October 2023	Review Date:	October 2024	Authorised By:	Paul Flynn
--------	---	-------------	--------------	--------------	--------------	----------------	------------



Section 11 – Data Retention Policy

Document	Retention Period	Legislation / Reference
Accounts Information	6 years from the end of the financial year in which the transaction was made	Companies Act
Bank Statements	6 years from the end of the financial year in which the transaction was made	Companies Act
Payroll Information	6 years from the end of the financial year in which the transaction was made	Pension Act, Taxes Management Act, Companies Act
Medical Records	40 years	HSE
Accident Records	3 years after the last entry or end of investigation if later	The Reporting of Injuries, Diseases and Dangerous Occurrence Regulations 1995
Personnel Files	6 years after the Employment Cease	Limitations Act 1980 and Data Protection Act 1998
Recruitment Information	12 Months	One-year limitation for defamation actions under Limitations Act
Leases	12 years After the lease and Liabilities under the lease have terminated	Limitations Act 1980
Pension information	Permanently	Companies Act, Commercial, Pension Act
Insurance Certificates	40 years	Employers Liability Regulations 1998
Board Meeting mins, Shares, Dividends	Permanently	Companies Act
Directors Service Contracts	Permanently	Companies Act
Major Agreements of historical Significance	Permanently	Data Protection 1998
H&S Records	3 years for general records	HSE
H&S Hazardous Substances – COSHH Register	Until Revised with the exception of Asbestos which is 40 years	HSE
Main Contractor Contracts	12 years	Limitations Act 1980
Contract Site Files	12 years post Project completion in line with Main Contractor Contracts	SCS Procedure
Disposal Records	3 years	HSE
Maintenance Records	5 years	HSE
Subcontractor Induction	40 years	HSE, Occupational Health Details

Distribution

This document will be made available as a source of reference to all staff. All persons employed by SCS Building Solutions Ltd are required to read and understand this policy.