

## Data Protection Policy

### Introduction

Student Christian Movement is committed to being transparent about how we collect and use the personal data of our workforce, and to meeting our data protection obligations in accordance with the General Data Protection Regulations (GDPR) and domestic laws. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, casual workers, contractors, volunteers, trustees, beneficiaries, donors and interns, and former employees and other personal data processed for business purposes. These are referred to in this policy as relevant individuals.

This policy is not contractual but indicates how Student Christian Movement intends to meet its legal responsibilities for data protection. We reserve the right to vary, replace or withdraw this policy at any time.

### Contents

[Definitions](#)

[Data protection principles](#)

[Roles and responsibilities](#)

[Types of data held](#)

[Individual rights](#)

[Subject access requests](#)

[Other rights](#)

[Data disclosures](#)

[Data security](#)

[Data monitoring](#)

[Privacy Impact Assessments](#)

[Direct marketing](#)

[Data breaches](#)

[International data transfers](#)

[Automated decision making](#)

[Third parties, contractors and self-employed persons](#)

[Training](#)

[Implementation, monitoring and review of this policy](#)

[Appendix 1 – Subject Access Request Procedure](#)

[Appendix 2 – Procedure for reporting data breaches](#)

[Appendix 3 – Document retention guidelines](#)

[Appendix 4 - SCM Confidentiality agreement](#)

## Definitions

"Data" is information which is processed or is intended to form part of a filing system. This applies to electronic or hard copy formats.

"Data Subject" is any identifiable, natural, legal person.

"Personal data" is any information that relates to an individual who can be directly or indirectly identified from that information.

"Processing" is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric and genetic data (where used for ID purposes).

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

## Data protection principles

Student Christian Movement processes personal data in accordance with the following data protection principles:

- Personal data is processed lawfully, fairly and in a transparent manner
- Personal data is collected only for specified, explicit and legitimate purposes
- Personal data is processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing
- Personal data is accurate, and all reasonable steps are taken to ensure that inaccurate personal data is rectified or deleted without delay
- Personal data is kept only for the period necessary for processing
- Appropriate measures are adopted to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Student Christian Movement tells relevant individuals the reasons for processing their personal data, how we use such data and the legal basis for processing in our privacy notices. Individuals will be made aware of the nature and purpose of data processing either when they submit that data to us or on our first subsequent contact with that individual. This will be done via privacy notices or a link to the online privacy notice. The full data protection policy will be made available on

request. Personal data of relevant individuals will not be processed for other reasons.

Student Christian Movement may process special categories of personal data or criminal records data when:

- Processing is necessary to carry out obligations and specific rights of the controller or relevant individual
- Processing is necessary to protect the vital interests of the relevant individual
- Processing is necessary for the purposes of the assessment of the working capacity of the relevant individual
- The relevant individual has given explicit consent to the processing of personal data.

Student Christian Movement will update personal data promptly if a relevant individual advises that their information has changed or is inaccurate.

Student Christian Movement keeps a record of its processing activities in respect of personal data in accordance with the requirements of the GDPR.

## Roles and responsibilities

### *Data Controller*

Student Christian Movement's Data Controller is the Chief Executive Officer. Their contact details are: [CEO@movement.org.uk](mailto:CEO@movement.org.uk) | 0121 426 4918

The Data Controller is the key decision maker in respect of why and how personal data is used and handled. The Data Controller will ensure that, both in the planning and implementation phases of processing activities, data protection principles and appropriate safeguards are addressed and implemented and that records of processing activity are kept. The Data Controller will also ensure that Privacy Impact Assessments are carried out, when necessary.

### *Data Processor*

These roles process personal data on behalf of, and further to, documented instruction given by the Data Controller. They are responsible for taking all measures required to ensure their own compliance with data protection legislation, and to immediately inform the Data Controller if they believe that any instruction given would be in breach of data protection legislation.

Processors are not permitted to appoint another processor without prior written agreement from Student Christian Movement. Equally, when we act as a processor

we will not appoint another processor without written agreement of the Data Controller we act on behalf of.

### Types of data held

Personal data gathered from beneficiaries, donors or others with whom we interact is held on a password protected database.

Personal data gathered during the working or volunteering relationship with Student Christian Movement is held in the individual's personnel file (in hard copy and/or electronic format), and on the electronic HR file. The periods for which HR related personal data is held can be found in the retention periods document included as an appendix to this policy.

The following types of data may be held by Student Christian Movement as appropriate, on relevant individuals:

- Name, address, phone numbers, emails – for the relevant individual and their next of kin
- Application forms and other information gathered during recruitment and selection procedures
- References from former employers, education establishments and/or personal referees
- National Insurance numbers
- Tax codes
- Job title, job description and pay details
- Terms and conditions of employment
- Conduct and/or capability issues such as letters of concern, improvement notes, disciplinary proceedings
- Holiday records
- Performance management information, such as supervision notes, appraisals, performance development plans
- Medical or health information
- Sickness absence records
- Training records

Personal data relating to criminal convictions and offences shall be handled with a greater level of protection than that which is applied to standard personal data.

Student Christian Movement will only process criminal records data, e.g. a criminal records check, where there is a legitimate requirement to do so, namely in respect of our duties as an employer. Where there is a legal obligation for us to review or record such data, we may seek to establish the required information from the employee, worker, self-employed person, contractor or any third party.

### *Beneficiary records*

We hold personal information about our beneficiaries as part of our service provision to them. This includes their name, address and contact details, event bookings, membership information and links to groups, chaplaincies and churches affiliated to the movement. This information is used for a variety of administration and management purposes.

### *Donor records*

We hold personal information about our donors as part of our service provision to them. This includes their name, address and contact details, event bookings, membership information and details of their donations, bank details and gift aid declarations. This information is used for a variety of administration and management purposes.

## Individual rights

As a data subject, relevant individuals have a number of rights in relation to their personal data.

Relevant individuals have the right to be informed about how Student Christian Movement processes personal data about them and the reasons for processing. Student Christian Movement privacy notices explain what data we collect, how we collect and process it and the lawful bases relied on for processing. A separate privacy notice applicable to job applicants is also available.

If Student Christian Movement intends to use data already collected for a different reason than that already communicated, we will inform relevant individuals of the new reason in advance.

## Subject access requests

Relevant individuals have the right to access the personal data held on them by Student Christian Movement.

Further information on how to request access to personal data is available in Appendix 1.

## Other rights

Relevant individuals have a number of other rights in relation to their personal data.

They can require Student Christian Movement to:

- stop processing or erase data that is no longer necessary for the purposes of processing;

- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

To ask for any of these steps to be taken, the individual should send their request to the Data Controller. If the response to the request is that Student Christian Movement will take no action, this will be confirmed to the individual in writing.

### Data disclosures

Student Christian Movement may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include, but are not limited to:

- any employee benefits operated by third parties
- relevant individuals with disabilities – whether any reasonable adjustments are required to assist them at work
- individuals' health data – to comply with health and safety or occupational health obligations towards the employee
- Statutory Sick Pay purposes
- HR management and administration – to consider how an individual's health affects their ability to do their job
- The smooth operation of any employee pension plan.

Such disclosures will only be made when strictly necessary for the purpose.

### Data security

Student Christian Movement takes the security of personal data seriously. There are internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. Control measures include:-

- Databases are password protected and backed up on our server.
- HR files are stored in locked filing cabinets with controlled access to keys
- Electronic HR files are stored on the server requiring a separate login and are backed up on a secure device.

Personal data (special category or not) should only be transferred where it is strictly necessary for the effective running of the organisation. Employees must seek consent from their line manager before transferring special category data.

In addition, employees must:

- Ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- Ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- Check regularly on the accuracy of data being entered into computers
- Always use the passwords provided to access the computer system(s) and not abuse them by sharing with people who should not have them
- Use computer screen blanking to ensure that personal data is not left visible on the screen when not in use
- Ensure personal data is not kept or transported on laptops, tablets, USB sticks or similar devices, unless authorised by the Chief Executive Officer.

Where data transfers occur via physical media such as memory cards, USB sticks etc, they must only be dispatched via secure post such as Recorded or Special Delivery. The use of first or second class Royal Mail is not permitted. The recipient should be clearly stated on the parcel, and the item securely packaged so that it does not break or crack.

The recipient should be informed in advance that the data is being sent, and must confirm safe receipt as soon as the data arrives. The employee responsible for sending the data is responsible for confirming the data has arrived safely.

Where Student Christian Movement engages third parties to process personal data on our behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

### Data monitoring

Workplace monitoring will be carried out in order to fulfil our legal obligations as an employer as well as to aid effective business operations. Because monitoring includes the processing of employee data, and may intrude on individuals private lives, it will be carried out in accordance with the GDPR, and only when deemed necessary and justifiable for business purposes.

Student Christian Movement will uphold a degree of privacy at work and where monitoring is required or necessary, employees will be informed of the extent of any

monitoring, together with the reasons why monitoring is taking place. Access to information and data collected will be secure and restricted to authorised personnel.

### Privacy Impact Assessments

Some of the processing that Student Christian Movement carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the Data Controller will carry out a Privacy Impact Assessment (PIA) to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

### Direct marketing

SCM will treat the following unsolicited direct communication with individuals as marketing:

- seeking donations and other financial support;
- promoting any SCM services;
- promoting SCM events;
- promoting membership to supporters;
- promoting sponsored events and other fundraising exercises;
- marketing the products of SCM;
- marketing on behalf of any other external company or voluntary organisation.

Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and the individual will have to opt in to their data being used for marketing purposes. SCM does not have a policy of sharing lists, obtaining external lists or carrying out joint or reciprocal mailings.

SCM will only carry out telephone marketing where consent has been given in advance, or the number being called has been checked against the Telephone Preference Service.

Whenever e-mail addresses are collected, any future use for marketing will be identified, and the provision of the address made optional.

### Data breaches

If an employee discovers that data has been lost or is missing, they should refer to our procedure for reporting data breaches, set out in Appendix 2.



## International data transfers

Student Christian Movement will not transfer HR-related personal data to countries outside the EEA.

## Automated decision making

Individuals have the right not to have decisions made about them solely on the basis of automated decision making processes where there is no human intervention, where such decisions will have a significant effect on you.

Student Christian Movement does not make any decisions based on such processes.

## Individual responsibilities

Individuals are responsible for helping Student Christian Movement keep their personal data up to date. Individuals should let their manager know if data changes, for example if an individual moves house or changes their bank details.

Individuals may have access to the personal data of other individuals and of our beneficiaries in the course of their working with us. Where this is the case, individuals are required to help meet our data protection obligations to staff and beneficiaries.

Individuals who have access to personal data are required:

- to only access data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- to ensure the secure transfer of data (for example by gaining prior authorisation, using Recorded or Special Delivery and ensuring physical media is encrypted or password protected)
- not to store personal data on local drives or on personal devices that are used for work purposes.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under our Disciplinary Procedure. Significant or deliberate

breaches of this policy, such as accessing HR related or beneficiaries' data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to summary dismissal.

### Third parties, contractors and self-employed persons

If any third party, contractor or self-employed person is found to be failing to meet obligations with data protection laws then we may serve notice on the contract for services.

Serious, deliberate or negligent transgressions may lead Student Christian Movement to terminate the contract for services with immediate effect. In this event, all reasonable steps will be taken to recover and protect the personal data concerned. Where the rights and freedoms of data subjects are likely to be at risk, the data subjects will be notified without delay.

### Training

Student Christian Movement will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional information and support to help them understand their duties and how to comply with them.

### Implementation, monitoring and review of this policy

This policy will take effect from 8 June 2019. The Chief Executive Officer has overall responsibility for implementing and monitoring this policy, which will be reviewed on a regular basis following its implementation (at least annually) and additionally whenever there are relevant changes in legislation or to our working practices. Any additions or revisions to this policy will be communicated to employees where appropriate.

Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Data Controller. Any employee who considers that the policy has been breached in any way should raise the matter with the Data Controller or Chair of Trustees.

## Appendix 1 – Subject Access Request Procedure

### Introduction

Under the General Data Protection Regulation (GDPR), individuals have the right to receive confirmation that Student Christian Movement processes their personal data, and also a right to access that data so that they are aware of it and are able to verify the lawfulness of the processing. The process for doing so is called a Subject Access Request (SAR), and this document sets out the procedure to be undertaken when such a request is made by an individual regarding data processed about them by Student Christian Movement.

### What is personal data?

“Personal data” is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, including the individual’s name.

“Special categories of personal data” includes information relating to:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life or
- sexual orientation.

### Procedure

To make a SAR, the relevant individual should complete a Subject Access Request form and send to the Data Controller Including specific details of the data being requested will enable a more efficient response from us.

On receipt of a Subject Access Request Form, in some cases, we may ask for proof of identification before the request can be processed. The Data Controller will inform the relevant individual if their identity needs verifying and the documents required.

The Data Controller will then confirm:

- whether or not the relevant individual’s data is processed and if so why; the categories of personal data concerned and the source of the data if it is not collected from the relevant individual;

- to whom the relevant individual's data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long the relevant individual's personal data is stored (or how that period is decided);
- the relevant individual's rights to rectification or erasure of data, or to restrict or object to processing;
- the relevant individual's right to complain to the Information Commissioner if they think Student Christian Movement has failed to comply with their data protection rights; and
- whether or not Student Christian Movement carries out automated decision-making and the logic involved in any such decision-making.

The Data Controller will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless agreed otherwise. Only personal data relating to the relevant individual who made the request will be released.

Student Christian Movement will normally respond to a SAR within a period of one month from the date it is received by the Data Controller. In some cases, such as where we process large amounts of the individual's data, we may respond within three months of the date the request is received. The Data Controller will write to the individual within one month of receiving the original request to tell them if this is the case.

We will be unable to supply certain pieces of information, for instance where it is subject to legal privilege or relates to management planning. Where this is the case the Data Controller will write to the individual to inform them that the request cannot be complied with, and give an explanation for the reason.

Relevant individuals must inform the Data Controller immediately if they believe that the data is inaccurate, either as a result of a SAR or otherwise. We will write to the individual within one month of receiving the notification, unless the required correction is complex in which we may respond within three months. If the response is that no action will be taken, we will inform the individual of the reasons for this, and of their right to complain to the Information Commissioner.

In the event that inaccurate data was disclosed to third parties, we will inform the third party of the correction where possible, and also inform the individual of the third parties to whom the data was disclosed.

### **Refusing a SAR**

If a SAR is manifestly unfounded or excessive, or repetitive, we are not obliged to comply with it. If an individual submits a request that is unfounded or excessive, or

to which we have already responded, the Data Controller will notify the individual that this is the case and whether or not we will respond to it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. We will inform the individual of their right to complain to the Information Commissioner.

### **Enforced SARs**

Forcing individuals to obtain information about themselves via a SAR, usually in relation to their criminal record, is a criminal offence. No individual will be required to make a SAR to another organisation, e.g. ACRO Criminal Records Office, HM Prison Service, HM Courts and Tribunal Service or the Crown Prosecution Service, in relation to any aspect of their recruitment, selection or ongoing employment with Student Christian Movement.

In the event we require information about an individual's criminal record, we will request this information in accordance with our Safeguarding Children and Vulnerable Adults Policy and associated appendices.

## Subject Access Request Form

You should complete this form to make a subject access request, which means you are asking Student Christian Movement to confirm to you that it processes your personal data, and to obtain access to that data.

Personal details	
Your name:	
Home address:	
Telephone number:	
Email address:	
Information sought	
<p>Please use the space below to describe, in as much detail as possible, the information you wish to have access to. If appropriate, please include any dates relevant to the information sought.</p>	
Declaration	
<p>I confirm that I am the person named above and the information requested above is in relation to me. I understand that I may be required to provide evidence to verify my identity.</p>	
Your signature:	
Date:	

## Appendix 2 – Procedure for reporting data breaches

### Introduction

Student Christian Movement is fully aware of its obligations under the General Data Protection Regulation (GDPR) to process data lawfully and to ensure it is kept securely. We take these obligations extremely seriously and have protocols in place to ensure that, to the best of our efforts, data is not susceptible to loss or other misuse.

The GDPR incorporates a requirement for a personal data breach to be notified to the supervisory authority and in some cases to the affected individuals. This procedure sets out Student Christian Movement's stance on taking action in line with GDPR if a breach occurs.

### Personal data breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed. A 'breach', for these purposes, is identifiable as a security incident which has affected the confidentiality, integrity or availability of personal data.

As indicated above, a data breach for these purposes is wider in scope than the loss of data. The following are examples of data breaches:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a data controller or data processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

### Breach detection measures

We have implemented the following measures to assist us in detecting a personal data breach:

Data protection agreements with third parties who act as data processors for us; provision of regular training on GDPR compliance for current employees, and covered during induction of new staff; alerts are received if someone logs in to the database from a different computer as a security measure

We may also become aware of a personal data breach from a member of staff, a beneficiary, a member of the public etc.

## Notifiable breaches

For the purposes of this procedure, a data breach will be notifiable when it is deemed by Student Christian Movement as likely to pose a risk to people's rights and freedoms. If it does not carry that risk, the breach is not subject to notification although it will be entered on our breach record.

A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

When assessing the likelihood of the risk to people's rights and freedoms, we will consider:

- the type of breach
- the type of data involved including what it reveals about individuals
- how much data is involved
- the individuals involved e.g. how many are involved, how easy it is to identify them etc
- how bad the consequences for the individuals would be and
- the nature of our work and the resultant severity of a breach.

## Reporting a breach

If an employee identifies a data breach, they must inform their line manager immediately, who will refer the matter to the Data Controller. An investigation will be initiated to establish the events leading to the breach, and determine what actions should be taken to restrict any consequences. A decision will be taken at that point about whether the breach is deemed notifiable, and whether it is deemed as resulting in a high risk to the rights and freedoms of individuals.

If there has been a data breach that poses a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of discovery. If notification is made beyond this timescale, we will provide reasons for this. If it has not been possible to conduct a full investigation into the breach within 72 hours, an initial notification of the breach will be made within 72 hours, giving as much detail as possible, together with reasons for incomplete notification and an estimated timescale for full notification. The initial notification will be followed up by further communication to the Information Commissioner to submit the remaining information.

The following information will be provided when a breach is notified:

- a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned and



- the categories and approximate number of personal data records concerned
- the name and contact details of the Data Controller where more information can be obtained
- a description of the likely consequences of the personal data breach and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

The Police may also be informed if it is found that unauthorised individuals have unlawfully accessed special category data that has been kept securely within the organisation.

If a notifiable breach has occurred which is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals as soon as possible that there has been a breach and provide them with the following information:

- a description of the nature of the breach
- the name and contact details of the Data Controller where more information can be obtained
- a description of the likely consequences of the personal data breach and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

### **Record of breaches**

The Data Controller will record all personal data breaches regardless of whether they are notifiable or not, as part of our general accountability requirement under GDPR. We will record the facts relating to the breach, its effects and the actions taken.

## Appendix 3 – Document retention guidelines

SCM's document retention guidelines are listed below and encompass both the legal requirements and our organisation's specific requirements. We will review data regularly and ensure that old data is identified and removed and destroyed safely. We will add data types to this list as and when appropriate.

The Data Protection Act states that personal files should not be kept "longer than necessary" but does not define this concept. Some statutory retention periods are dictated by legislation; where there are no statutory retention periods we will follow recommended retention periods.

Documents	Recommended retention period	Comments
<b>Beneficiary records</b>		
Contact information, event attendance and membership records (inc graduation date and place of study).	Permanently	Where people have asked for their contact details not to be used, a person is marked as never mail on the database. Their records are kept to prevent someone being re-added at a later date.
Medical information disclosed at an event.	Until the end of the event.	Participants have the option of completing a medical form which is placed into a sealed envelope, and can be given to medical personnel in case of an emergency. The lead staff member should keep these confidential and shred immediately after the event.
Any other records	Up to three years after the membership end date	Information such as denomination and access requirements.
<b>Donor records (some beneficiaries are also donors)</b>		
Donation information, including gift aid declarations	six years after the tax year end	Required in case of an audit. Gift aid declarations must have a clear link between the donation and donor.
<b>Human Resources</b>		
Employee personnel & training files	Six years after employment ceases	Health and Safety records may need to be kept longer (see below)
Senior executive records e.g. senior management team and/or Trustees	Permanently	

Details of redundancy calculations, payments	Six years after employment ceases	
Unsuccessful job applications - forms and interview notes	One year following date of notification	Three months for a tribunal claim on grounds of discrimination (although can be extended by tribunal). One year limitation for defamation actions.
Time cards/records	Two years following audit	Working Time Regulations 1998
Expense accounts	Six years following year end for public companies	Companies Act 1985, section 222
Statutory sick pay records, calculations, certificates, self-certificates	Three years after end of tax year to which they relate	Statutory Sick Pay (general) Regulations 1982
Annual leave records	Two years	
Appraisals	Two years	
Discipline and grievance records	May not be used once duration of warnings is spent, but should be retained for two years	Transfer of Undertakings (Protection of Employment) Regulations 2006
Maternity leave and pay records	Three years after end of tax year in which the maternity period ends	Statutory Maternity Pay (General) Regulations 1986
Parental leave	Five years from birth/adoption of the child or 18 years if the child receives a disability allowance	
<b>Pensions</b>		
Records relating to notifiable events and concerning decisions to allow retirement due to incapacity, pension accounts and associated documents	Six years from the end of the scheme year in which the event took place or the date upon which the accounts/reports were signed/completed.	Retirement Benefits Schemes (Information Powers) Regulations 1995
Pension scheme investment policies	Twelve years from the ending of any benefit payable under the policy	
Pensioners records	Twelve years after benefit ceases	
Actuarial valuation reports	Twelve years after benefit ceases	
Money purchase details	Six years after transfer or value taken	

Trust deeds and rules	Permanently	
<b>Health &amp; Safety</b>		
Accident books, records and reports	Three years after the date of the last entry	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended
Health and Safety records	Forty years	Personal injury claims must normally commence within three years of injury. However this period may be substantially extended for industrial injuries which are not capable of being detected in less than three years.
Risk assessments and records of consultations with safety reps and committees	Permanently	Best practice
<b>Medical records</b>		
Medical records as specified by COSHH regulations	Forty years from date of last entry	COSHH Regulations 1999 and 2002
Records of tests and examinations of control systems and protective equipment under the COSHH regulations	Five years from date of the test	COSHH Regulations 1999
Medical records as specified by the Control of Asbestos at Work Regulations	Forty years from date of last entry (four years from the date of issue for medical examination certificates)	Control of Asbestos at Work Regulations 1987 and 1998
Medical records as specified by the Ionising Radiations Regulations	Until the person reaches the age of 75 but in any event at least 50 years	Ionising Radiations Regulations 1999
<b>Accounting records</b>		
Accounting records	Three years for private companies, six years for plcs	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
Inland Revenue approvals	Permanently	
Wage/salary records (including overtime, bonuses and expenses, other payment records including statutory payments, working tax credit, NMW, payments to subcontractors, gains on share options and student loan deductions)	Six years following year end	Taxes Management Act 1970 Income Tax (Employments) Regulations 1993 and Income Tax (Pay As You Earn) Regulations 2003

## Appendix 4 - SCM Confidentiality agreement

This agreement is between SCM and \_\_\_\_\_ (individual's name)

### Introduction

During the course of your relationship with SCM you will see and obtain confidential information which relates to SCM and/or our beneficiaries.

In signing this agreement, you agree to abide by rules set out below regarding confidentiality. You agree:

- to keep all confidential information to which you have access secret and confidential and not to disclose it to anyone (except workers of SCM or other authorised people as may be necessary in the proper course of any work you undertake for us or on our behalf). This applies to all confidential information, whether communicated verbally, in writing or otherwise;
- not to use the information for any purpose without obtaining our prior written agreement;
- if we request it, to return any documents or items connected with any work you undertake for us on our behalf, and not to retain any unauthorised copies.

### Definition of "Confidential Information"

"Confidential Information" includes all information, whether in writing or not, including but not limited to documents, descriptions, research, service developments, financial information and computer software. This includes, in particular, information belonging to or relating to:

- details of our beneficiaries and prospective beneficiaries, and
- all other information which will reasonably be regarded as confidential in the context of our organisation.

### Limitations on the use and disclosure of Confidential Information

To help secure the confidentiality of the above, you agree that you will:

- keep all confidential information separate from other documents and records of SCM
- not remove any "Confidential Information" stamps or marking appearing on such confidential information and take all reasonable steps to preserve the confidentiality of such information

- not disclose confidential information to workers of SCM other than those authorised to receive such information, e.g. those who have a need to know and whose knowledge is necessary to deliver the agreed services
- not communicate confidential information to any third party unless you have our written authority. In addition you will use your best efforts to prevent inadvertent disclosure of the confidential information to any third party.
- only copy, reproduce and transform confidential information to the extent that is strictly required for the purpose of providing the agreed services
- not use any confidential information for any purpose without our prior written consent except as necessary for:
  - carrying out the agreed services in a professional manner
  - negotiations, discussions and consultations with employees or workers acting on behalf of SCM
  - any other purpose we may authorise in writing.

It is not the intention of this Agreement to prevent you from using your own personal skill and knowledge in any business in which you may lawfully be engaged, interested or concerned after the termination of this Agreement.

## Exclusions

The obligations on using and disclosing confidential information do not apply to any information which:

- you can prove by written record was in your possession free of any obligation of confidence at the time of our communication of it to you
- is or becomes publicly known through no wrongful act on your part
- is disclosed to you without any obligations of confidence by a third party without breach of this Agreement
- was subsequently independently developed without reference to any of the confidential information or other information that we have disclosed in confidence to you
- is required to be disclosed to any government body or other authority as required by law
- is approved for release or use by written authorisation of SCM.

## Responsibility

You will be responsible for any breach of confidentiality or any misuse of confidential information by any parties related to you or any other party to whom you disclose the confidential information.

## Return of Confidential Information

You shall return all confidential information and all copies of such information disclosed to you by SCM following termination of this Agreement.

Upon written request by either you or SCM the other party shall provide a signed, dated receipt which itemises the confidential information transmitted or received.

Signed by: ..... Date: .....  
On behalf of SCM

Signed by: ..... Date: .....  
Individual

One copy to be retained by the individual and one copy to be retained by SCM.