INTO UNIVERSITY PARTNERSHIPS LIMITED – GUIDANCE TO EMPLOYEES - HANDLING SPECIAL CATEGORY PERSONAL DATA AND DATA IN RELATION TO CRIMINAL CONVICTIONS

1. INTRODUCTION

1.1 In the course of INTO's business, we regularly deal with special category personal data (as defined below), and personal data which relates to criminal convictions. The purpose of this Guidance is to explain the legal requirements for handling this type of data, and to set out the standards we need to apply when we do so.

1.2 This Guidance applies to special categories of personal data of both INTO employees and students. We understand that this kind of personal information can be genuinely sensitive, and our employees and students want to know we will treat it with the utmost care and appropriate confidentiality.

1.3 Under the General Data Protection Regulation (the "GDPR"), we are "controllers" in relation to the personal data that we collect, use, store, or do anything else with (anything we do with personal data is known as "processing"). As controllers we decide what personal data is processed, why it is processed, why (legally) we have a right to process the personal data and how it is processed. As controllers, we have the legal responsibility to ensure that personal data, including special category data, is looked after in accordance with data protection law.

1.4 Whilst this Guidance and Policy is directly relevant to our employees in the UK whose handling of data is subject to the GDPR, it is also relevant to our employees outside Europe who handle the personal data of people who are inside the EU or who use systems which process personal data in the EU, for example, Salesforce. Furthermore, whilst globally there are different laws and regulations which deal with the protection of personal data, we consider the GDPR to be a good minimum standard for us to adhere to in our operations across the world.

2. WHAT IS SPECIAL CATEGORY PERSONAL DATA?

2.1 Special category personal data is defined in the GDPR as:

"personal data which reveals **racial or ethnic origin**, **political opinions**, **religious or philosophical beliefs** or **trade union membership**. It also includes **genetic data**, **biometric data**, and data concerning **health**, a person's **sex life** or **sexual orientation**."

Prior to the introduction of the GDPR (under the Data Protection Act 1998) these categories of personal data were known as "sensitive personal data". Under GDPR, special category data is afforded additional protection because it is deemed to be so sensitive.

2.2 We are unlikely to process some of these special categories of personal data on a regular basis, if at all, but we need to be aware of what constitutes special category data so we can apply the appropriate protections when processing it. We do, however, deal routinely with certain categories of special category personal data. For example, we ask every potential student for information about any disabilities they may have, so we can make whatever reasonable adjustments are necessary to enable disabled students to study at one of the centres. We ask employees about their racial or ethnic origin for the purposes of equal opportunities monitoring. HR keep health and sickness records relating to employees to manage sickness absences and process records relating to trade union membership.

2.3 In order to be compliant in our data processing, we need to make sure that all our processing activities are necessary, have a legal basis, are supported (in most cases) by an appropriate policy document (further details below), and that we are transparent about what we are doing and why we are doing it.

3. PERSONAL DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES

3.1 As well as special category data, we also process certain "criminal conviction data" in relation to both students and employees.

3.2 This kind of personal data is also given particular protection under GDPR, for similar reasons to the protection given to special category data. The rules for processing criminal offence data are separate to the special category data rules, but there is significant overlap.

3.3 Further guidance in relation to the handling of "criminal offence" data is provided at Paragraph 6 below.

4. PROCESSING SPECIAL CATEGORY DATA – LEGAL BASIS

4.1 As with the processing of all personal data, when we process special category data, we must first have a lawful basis for doing so. This is known as the “Article 6 basis”. A list of all Article 6 bases can be found here: https://gdpr-info.eu/art-6-gdpr/

4.2 One Article 6 basis is “consent”. However, consent to processing should be a genuine choice. Guidance from the Information Commissioner’s Office (the ”ICO”, the regulator for data protection in the UK) states “*if you would still process the personal data without consent, asking for consent is misleading and inherently unfair*”. Consent is only one lawful basis for processing and is not always the most appropriate or easiest basis to rely on, particularly given an individual can withdraw their consent to the processing at any time. We therefore only rely on consent where this is specifically required by law, for example, in relation to our direct marketing activities.

4.3 We also rarely rely on the "vital interests" basis (which is aimed at life or death situations, for example, providing a student's personal data to emergency services), or the ”public interest” basis (which is more commonly used by public authorities, for example, by our university partners).

4.4 This, therefore, leaves the bases of "contract", "legal obligation" and "legitimate interests" as the bases we most often rely on for our processing of personal data, including special category data. GDPR requires us to keep a Record of Processing Activity ("ROPA") which documents all of the processing activities we undertake and identifies our legal basis for each activity. The ROPA is maintained by our DPO, Veronica Morrison. If you have any queries relating to the ROPA, please contact veronica.morrison@intoglobal.com You should also contact the DPO each time a new processing activity is undertaken or an existing processing activity is amended to ensure the ROPA is accurate and up to date in terms of all our processing activities.

5. ADDITIONAL LEGAL CONDITIONS

5.1 In addition to identifying an Article 6 basis required to process any and all personal data, to process special category personal data we also need to meet a further legal basis as set out in the GDPR. This is known as the “Article 9 basis”: https://gdpr-info.eu/art-9-gdpr/. Depending on which Article 9 basis is appropriate, we may also still need to satisfy a further condition as set out in Schedule 1 of the Data Protection Act 2018 (the "DPA"), and as described in paragraphs 5.3 and 5.4 below.

5.2 The Article 9 bases for the processing of special category data are summarised below:

(a) Explicit consent;

(b) Necessary for the purposes of employment, social security and social protection;

(c) Protection of vital interests;

(d) Processing carried out by not-for-profit bodies;

(e) Data made public by the data subject;

(f) Legal claims;

(g) Substantial public interest;

(h) Preventative or occupational medicine, health or social care;

(i) Public health;

(j) Archiving in the public interest, scientific or historical research.

5.3 If we are relying on bases (b), (g), (h), (i) or (j) the DPA states the processing must still meet further conditions, which are set out in Schedule 1 of the DPA. While Schedule 1 sets out a large number of "substantial public interest" conditions that can be relied on, very few will be relevant to the purposes for which we would normally process special category personal data. Additionally, they are narrow in their application. Further, if we rely on the “substantial public interest” basis, we must have an “appropriate policy document” in place. Our “appropriate policy document” is attached to this Guidance at Appendix 1 (the "Policy"). Our ROPA also needs to confirm which Article 9 bases we are relying on for each processing activity that relates to the processing of special category data.

5.4 Our "appropriate policy document" explains our procedures for complying with the data protection principles set out in the GDPR and identifies the appropriate Schedule 1 condition for each of our activities involving the processing of special category data.

6. PROCESSING CRIMINAL OFFENCE DATA – LEGAL BASIS

6.1 As stated above, under the GDPR, we can only process personal data (of any type) if we have a lawful Article 6 basis to do so.

6.2 In addition to having an Article 6 basis, the processing of personal data relating to criminal convictions and offences must be specifically authorised by law.

6.3 As with the processing of special category personal data, this authorisation can be found in the DPA, which sets out the limited, specific set of circumstances in which such processing is authorised. All of the Schedule 1 conditions for the processing of special category data are available (paragraphs 1-28), as well as the additional conditions set out below:

Paragraph	Condition relating to
29	Consent
30	Protecting individual’s vital interests
31	Processing by not-for-profit bodies
32	Personal data in the public domain

33	Legal claims
34	Judicial acts
35	Administration of accounts used in commission of indecency offences involving children
36	Extension of conditions in Part 2 referring to substantial public interest
37	Extension of insurance conditions

6.4 The rules for processing criminal offence data are similar to those set out above for processing special category data including having an "appropriate policy document" in place.

6.5 When we process criminal offence data, we will usually rely on either the conditions relating to employment, social security and social protection, a statutory purpose, or when we consider the processing to be necessary for the purposes of the prevention or detection of an unlawful act.

6.6 It is unlikely we would seek the consent of either students or employees (except in very limited circumstances) in order to process criminal offence data. As noted above consent requires careful management and should only be sought where there is an intention to offer the data subject a genuine choice and where we are confident the data subject will not withdraw their consent to the processing.

7. CRIMINAL OFFENCE DATA IN RELATION TO STUDENTS

7.1 We only collect criminal offence information in relation to students where there is a specific and proportionate need for us to do so, for example, in relation to the issuance of a CAS. Relating to this, UCAS no longer asks all applicants to declare any relevant unspent criminal convictions, but still asks applicants of courses which lead to professions which are exempt from the Rehabilitation of Offenders Act 1974 to make such a declaration.

7.2 Given the high threshold we are required to meet to process data relating to criminal convictions, we need to be certain that we have a good reason to ask applicants to provide this information to us. As noted above, we need to satisfy an Article 6 basis, an Article 10 basis and a condition from Schedule 1 of the DPA. If we have a mandatory statutory obligation to process criminal offence data, for example, because it is a requirement of the Immigration Rules, we may rely on the Article 6 basis, where the "processing is necessary for compliance with a legal obligation to which the controller is subject", and on the relevant provisions of the DPA where the processing is necessary "for the exercise of a function conferred on a person by an enactment or the rule of law".

7.3 There may also be circumstances in which we process criminal offence data where we have a non-mandatory statutory basis for doing so, in reliance on the Article 6 basis where the "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller." Although this basis is more often relied upon by public authorities, it may be relevant for us if we can reasonably say that any of the activities for which we are processing criminal offence data are in the public interest, for example where it is necessary for the prevention or detection of an unlawful act.

7.4 As with all personal data we process, including special category personal data, we need to identify each processing activity relating to criminal offence data and record it in our ROPA, together with the lawful Article 6 basis and the additional condition under the DPA.

7.5 We may also ask applicants to provide us with criminal offence data when we have wider safeguarding concerns. This might happen in centre, for example, in connection with a particular type of accommodation. We will only ask for a

declaration of criminal offence data once a student has accepted an offer of accommodation (or in relation to whichever stage of the student journey for which such data may be relevant).

8. CRIMINAL OFFENCE DATA IN RELATION TO EMPLOYEES

8.1 We process information in relation to criminal convictions and offences only in the context of the recruitment for and management of certain posts, for example teaching and other roles where unaccompanied contact with minors is required, or in relation to certain roles in Finance, Human Resources or Legal. This is because posts of this nature may require a Criminal Records Certificate, or an Enhanced Criminal Records Certificate. We may also process such information in certain other scenarios where our employees may come into contact with students (for example, where a security pass may be required to access a building where students are present).

8.2 We ask applicants for these posts (and employees who may otherwise come into contact with minors) to submit personal data to a third-party provider which carries out a check with the Disclosure and Barring Service (DBS). In the case of applicants who are applying for a job with us, a DBS check is only made to a preferred candidate once we have made a conditional offer of employment and which is subject to a satisfactory DBS check or equivalent in Northern Ireland and Scotland. The successful applicant is sent a link from HR which they open to submit their personal data prior to verification of the original documents between the employee and HR. When the check has been completed, both we,(via HR) and the applicant, are notified if there is any "content on record".

8.3 If we are notified that there is "content on record", we will contact the applicant to ask for more detailed information. If an applicant is unwilling to provide us with this information, it is likely that any offer of employment will be withdrawn.

8.4 When we process this data, we do so on the basis that it is necessary for us to comply with a legal obligation (our Article 6 basis), and it is necessary for the purpose of exercising our rights (or performing our obligations) as a controller in connection with employment (our Schedule 1 condition). We do not rely on consent as the basis for this processing.

9. INFORMATION SECURITY

9.1 We are committed to the highest standards of information security when processing any personal data.

9.2 In relation to all personal data, including special category and criminal offence data, the GDPR requires us to:

9.2.1 use technical or organisational measures to ensure personal information is kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage;

9.2.2 implement appropriate technical and organisational measures to demonstrate that we have considered and integrated data compliance measures into our data processing activities; and

9.2.3 be able to demonstrate that we have used or implemented such measures.

9.3 Employees should ensure they are familiar with our Information Security Policies and apply best practice guidance to establish and maintain appropriate security

arrangements and technical and organisational measures for the type of personal data they access in the course of their work.

9.4 Keeping personal data safe is a responsibility for all of us. For further information, please refer to these IT policies:

9.4.1 Information Security Policy;

9.4.2 Acceptable Use of IT Policy;

9.4.3 Asset Management Policy; and

9.4.4 Data Transfer Policy

Copies of these can be found in the Information Security and Technology Use sections on INTONET / Policies

9.5 In addition to the above, INTO is currently developing a Data Retention Policy with a Data Retention Schedule which will specify the different retention periods for different types of data, both personal and non-personal, held within the organisation. This will be circulated once finalised and training will be provided as required. Please keep an eye out for further information in this regard.

9.6 **Computers and IT**

9.6.1 We ensure that password protection and encryption is used where available on our systems and equipment in order to maintain confidentiality.

9.6.2 When a password protected document is sent or otherwise made available, the password must be sent to the recipient of the document by separate means, for example, by text. Spreadsheets and other documents containing personal data must always be password protected before they are shared.

9.6.3 Computers and other electronic devices must be password protected and those passwords must be changed on a regular basis or when required to do so by the IT department. Passwords must not be written down or given to others.

9.6.4 Computers and other electronic devices must be locked when not in use and when you leave your desk, to minimise the risk of accidental loss or disclosure. Equipment must be kept safe when in public areas to avoid theft or damage.

9.6.5 Confidential information and personal data must not be copied onto an external storage medium such as USB stick, CD/DVD, or uploaded to a Cloud storage/sharing service that has not been provided by INTO's IT team

9.6.6 Employees must ensure they do not introduce viruses or malicious code on to company systems. Software must not be installed on INTO equipment or downloaded from the internet without prior approval from the IT team. Employees should contact **Dave Colwell – dave.colwell@intoglobal.com** for guidance on appropriate steps to be taken to ensure compliance.

9.6.7 Mobile/cell phones or Tablets provided by the organisation must be kept locked when not in use and be safe and secure by either PIN or biometric security. When in public areas devices must be kept secure to avoid theft.

9.7 **Personal email and cloud storage accounts**

9.7.1 Cloud file storage solutions that are not provided by INTO's IT team must not be used, these include, but are not limited to, Google, Yahoo, OneDrive (Personal), DropBox, iCloud and, in addition, online large file sharing services. These solutions do not provide the level of security necessary for INTO's document sharing and collaboration requirements.

9.7.2 Email solutions not provided by INTO's IT team must not be used for any INTO business. All email communications must be conducted using the provided 'intoglobal.com' email account.

10. HUMAN RESOURCES INFORMATION

10.1 Given the internal confidentiality of personnel files, access to such information is limited to the HR Department although certain elements of an employee's records are also visible to line managers. Except as provided in individual roles, other employees are not authorised to access that information.

10.2 Any employees in a management, supervisory or Human Resources role or involved in recruitment must keep personnel data strictly confidential.

10.3 We handle requests from employees for access to their personal data in accordance with our employee privacy policies:

10.3.1 Global Privacy Notice for Employees and

10.3.2 CCPA Privacy Notices for Employees.

11. TRAINING

11.1 All employees will receive training on the key principles of data protection legislation to help them understand how their role may be affected and what their data protection responsibilities are. New joiners will be required to complete our online data protection training as part of the induction process run by HR. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policies and procedures.

11.2 The DPO will continually monitor training needs but if you feel that you need further training on any aspect of the relevant data protection law or our Information Security policies, please contact the DPO.

12. REPORTING DATA BREACHES

12.1 All of us have an obligation to report actual or potential data protection breaches. This allows us to:

12.1.1 investigate the incident and take remedial steps if necessary;

12.1.2 maintain a register of such incidents as required by current data protection laws; and

12.1.3 make any applicable notifications to the Data Protection Regulator.

12.2 Please report any actual or suspected personal data breaches or related incidents to your line manager and the DPO as soon as you become aware that there is or may be such an issue. Please complete the online Data Breach Report Form and refer to:

12.2.1 Guidance on Data Breaches & Reporting.

INTO UNIVERSITY PARTNERSHIPS LIMITED – APPROPRIATE POLICY DOCUMENT – SPECIAL CATEGORY AND CRIMINAL OFFENCE DATA

1. In the course of our business, we need to process both Special Category ("**SC**") data and Criminal Offence ("**CO**") data. When we undertake such processing we comply with the General Data Protection Regulation (the "**GDPR**") and the Data Protection Act 2018 (the "**DPA**") as well as any further laws, codes of practice or guidance in relation to processing personal data and privacy which are either enacted or published by a relevant supervisory authority and which are applicable to us from time to time.

2. Specifically, our processing of SC and CO data complies with Articles 9 and 10 of the GDPR, Schedule 1 of the DPA, and the data protection principles set out in the GDPR. The purpose of this policy document is to explain how our processing of this kind of data is consistent, where applicable, with these articles, conditions and principles, as well as to tell you about the length of time we need to hold such data.

3. WHAT IS SC DATA?

3.1 Article 9 of the GDPR defines SC data as being personal data which includes or reveals:

3.1.1 Racial or ethnic origin;

3.1.2 Political opinions;

3.1.3 Religious or philosophical beliefs;

3.1.4 Trade union membership;

3.1.5 Genetic data;

3.1.6 Biometric data for the purpose of uniquely identifying a natural person;

3.1.7 Data concerning health; and

3.1.8 Data concerning a natural person's sex life or sexual orientation.

3.2 Article 10 of the GDPR covers the processing of personal data which relates to criminal convictions, criminal offences, or related security measures.

3.3 Data protection law says that we can only process SC data if one of the conditions in Article 9(2) GDPR and/or in Schedule 1 of the DPA applies. If we process CO data, then this too must be on the basis of one of the Schedule 1 conditions.

3.4 Most of the conditions for processing SC or CO data also require us to have this document in place (an "Appropriate Policy Document") which explains our procedures for compliance, and for the retention and erasure of the data.

4. DESCRIPTION OF THE DATA WE PROCESS

4.1 We process special category data about our employees, prospective employees and former employees, including medical data, data in relation to physical or mental health, passport details and details in relation to equal opportunities monitoring. In each case, we process this data because it is necessary for us to fulfil our obligations or exercise our rights as an employer.

4.2 We process CO data about our employees, prospective employees and former employees as a part of our background checks, or where we need to comply with a legal obligation.

4.3 We also process SC and CO data about our students and prospective students including medical data, data in relation to disabilities, physical or mental health, details in relation to equal opportunities monitoring and criminal convictions.

5. SCHEDULE 1 CONDITIONS

5.1 We rely on the following Schedule 1 conditions when we process SC data:

5.2 **Part 1, Schedule 1 – Employment, Health and Research etc**

5.2.1 **Paragraph 1(1)(a)** employment, social security and social protection.

Processing includes:

(a) employee health data, and the passport details of prospective employees in accordance with the above condition when we manage business travel and in connection with employee familiarisation trips;

(b) medical data, physical or mental health data and ethnicity data in accordance with the above condition to create and maintain a personnel file;

(c) health data in accordance with the above condition to determine absences from work in the context of payroll requirements, and for pension administration.

5.3 **Part 2, Schedule 1 – Substantial Public Interest Conditions**

5.3.1 **Paragraph 6(1)** and **(2)(a)** statutory, etc. purposes

Processing includes

(a) ethnicity data and other SC data in accordance with the above condition where we are required to monitor equality of opportunity;

(b) student and prospective student disability data in accordance with the above condition to ensure that we can make reasonable adjustments necessary to ensure equality of access to student accommodation;

(c) student and prospective student ethnicity data in accordance with the above condition in relation to compliance with visa conditions.

5.3.2 **Paragraph 8(1)** equality of opportunity or treatment.

5.3.3 **Paragraph 10(1)** preventing or detecting unlawful acts.

5.3.4 **Paragraph 18(1)** safeguarding of children and of individuals at risk.

5.4 We only process CO data where such processing is consistent with the following purposes in Parts 1 and 2 of Schedule 1:

5.4.1 **Paragraph 1(1)(a**) employment, social security and social protection.

(a) criminal conviction data in accordance with the above condition when we recruit employees.

5.4.2 **Paragraph 6(1)** and **6(2)(a)** statutory, etc. purposes.

(a) criminal conviction data to comply with our obligations under immigration law.

5.4.3 **Paragraph 10(1)** preventing or detecting unlawful acts.

6. PROCEDURES FOR COMPLYING WITH THE PRINCIPLES

6.1 The GDPR sets out a number of principles in relation to the processing of personal data. These are set out below, together with measures we have taken to ensure that our processing of SC and CO data is in compliance with them.

6.2 Accountability

6.2.1 The GDPR requires us not only to comply with the data protection principles set out below, but to be able to demonstrate that we comply with them.

6.2.2 We have adopted several measures to meet this accountability requirement, including:

(a) appointing a Data Protection Officer to oversee our compliance and to ensure that data protection is at the heart of our decision making;

(b) implementing and maintaining an accurate record of our processing activities;

(c) implementing technical and organisational measures to protect the personal data that we process;

(d) putting a process in place to ensure that appropriate agreements are in place with organisations with whom we share personal data;

(e) ensuring we have appropriate privacy policies in place, and that our processing is consistent with them; and

(f) carrying out, where necessary, data privacy impact assessments.

6.3 Principle (a): processing must be lawful, fair and transparent

6.3.1 GDPR states that processing must be lawful, fair and transparent. For processing to be lawful, it must be specifically consented to by the data subject, or be necessary for one of the reasons set out in Article 6 of the GDPR. If the processing relates to SC or CO data, one of the Schedule 1 conditions must also apply.

6.3.2 We have identified a lawful basis for our processing, and a further Schedule 1 condition where the processing involves SC or CO data.

6.3.3 We set out our lawful bases for our processing (and the further conditions on which we rely) in our privacy notices, in greater detail in our Record of Processing Activity, and in this document. Our privacy notices provide transparent information about our processing.

6.3.4 We only process personal data in ways people would reasonably expect and use data privacy impact assessments and legitimate interests assessments to ensure that our processing is fair.

6.3.5 We are open and honest when we collect SC or CO data and do not mislead people about how we use it.

6.4 **Principle (b): personal data must be collected for specific and legitimate purposes and processed in accordance with those purposes**

6.4.1 Our privacy notices explain the purposes for which we process personal data, and we do not process personal data for purposes other than these.

6.4.2 We process SC data and CO data only where it is necessary for the purposes set out in one of the Schedule 1 conditions.

6.4.3 We do not process personal data for purposes which are incompatible with the purposes for which they were originally collected (unless this is to comply with a legal obligation, or to exercise a function which is set out in law).

6.5 **Principle (c): personal data must be adequate, relevant and limited to what is necessary for the stated purposes**

6.5.1 We aim to ensure we have sufficient SC and CO data for the purposes set out in the Schedule 1 conditions above, but do not collect or otherwise process SC or CO data in excess of what we require for these purposes.

6.5.2 If the DPO becomes aware that personal data is provided to us which is not relevant for our purposes, we will require employees to erase it.

6.5.3 We use national guidance and take external advice to help us determine what information we need to process.

6.6 **Principle (d): personal data must be accurate and, where necessary, kept up-to-date**

6.6.1 We have processes in place to check the accuracy of the SC and CO data we hold, and we record the source of such data.

6.6.2 We correct any inaccuracies in the SC and CO data we hold when data subjects exercise their rights under Article 16.

6.6.3 We keep a record of any challenges to the accuracy of the personal data we hold.

6.7 **Principle (e): personal data must be retained for no longer than necessary**

6.7.1 We are considering how long we need to process the SC and CO data for to enable us to justify the retention period we decide upon.

6.7.2 As part of our Data Retention Policy and Schedule, we will implement reviews of the SC and CO data we hold and seek to erase it when it is no longer necessary for the purposes for which it was collected.

6.8 **Principle (f): personal data must be kept securely**

6.8.1 We use encryption and pseudonymisation where we consider it appropriate for the level of sensitivity of the SC or CO data that we are processing.

6.8.2 We have, and have implemented, an information security policy.

6.8.3 We train our employees in the secure handling of SC and CO data in particular, and personal data in general.

6.8.4 We limit access to personal data to those of our employees, agents, contractors and third parties to those who have a business need to know the information.

6.8.5 We ensure that organisations that process personal data on our behalf implement technical and organisational measures which are sufficient to ensure the security of the data being processed.

7. RETENTION AND ERASURE

7.1 As set out above, we aim to retain personal data only for as long as necessary to fulfil the purposes we collected it for, including satisfying any legal, accounting, or reporting requirements (for example, to comply with reporting requirements in relation to UK Visas and Immigration, or tax reporting requirements to HMRC). We may also retain personal data for a period after this time if it is necessary and relevant for our legitimate operations.

7.2 In some circumstances we may anonymise personal data (so that it can no longer be associated with an individual) for statistical purposes, in which case we may use this information indefinitely.

7.3 Once an employee, worker or contractor leaves the company we will retain or destroy SC or CO data in accordance with applicable laws and regulation.

7.4 Our retention and erasure procedures are further documented in our Data Retention Policy & Schedule.

8. REVIEW DATE

8.1 This Appropriate Policy Document will be reviewed annually.