General Data Protection Regulations Procedures

South Thames College Group Procedures

Purpose

1 This guidance note sets out the following procedures under the South Thames Colleges Group General Data Protection Policy.

2 The procedures include:

i Individual Rights (Sections A to H)
ii Contracts (Section I)
iii Documentation – Information Asset Register (Section J)
iv Data Sharing Agreement – Local Authorities (Section K)
v Data Protection Impact Assessments (Section L)
vi Data Breach Policy (Section M)

Appendices:

1. STCG Privacy Notice (students and other stakeholders)
2. Process for handling Individual Rights requests
3. Data Sharing Agreement for Local Authorities
4. Data Breach Investigation Form
5. STCG Privacy Notice (Staff)
6. Data Retention Policy

3 Queries about the procedures should be forwarded to the Compliance Manager or Data Protection Officer.

Section A: Right to be informed

4 The College will meet the right to be informed as follows:

- Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.
- STCG will provide individuals with information including: the purposes for processing their personal data, the retention periods for that personal data, and who it will be shared with. This is called 'privacy information'.
- **STCG Privacy Notice and information is set out at Appendix 1**.
- We will provide privacy information to individuals at the time that we collect an individual's personal data from them. The privacy information will be included in the enrolment form for students.

- Where we obtain personal data from other sources, we will provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month. If we obtain personal data from a source other than the individual it relates to, we provide them with privacy information:

    - within a reasonable of period of obtaining the personal data and no later than one month;
    - if we plan to communicate with the individual, at the latest, when the first communication takes place; or
    - if we plan to disclose the data to someone else, at the latest, when the data is disclosed.

- There are a few circumstances when we will not provide privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.

- We will provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language. We will ask for feedback on how effective the delivery of our privacy information is.

- We will regularly review, and where necessary, update the privacy information on an annual basis in line with the publication of government advice to FE sector. We will bring any new uses of an individual's personal data to their attention before we start the processing.

Section B: Right to access

5 The College will meet the right to access as follows:

- Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

- Individuals will have the right to obtain:

    - confirmation that their data is being processed;
    - access to their personal data; and
    - other supplementary information – this largely corresponds to the information that should be provided in the **STCG Privacy Notice**.

- The College will not generally charge for a Subject Access Requests. However, we may charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. We may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that we will charge for all subsequent access requests. The fee will be based on the administrative cost of providing the information.

- **An individual can make a request verbally or in writing.** Staff members receiving a request verbally will log the details of the request and forward the request to the Compliance Manger.

- **Details of the process for making a request including ID verification, timescales, fees and refusing requests are included at Appendix 2**

- In line with the Privacy Notice, the College only holds data relating to an individual's enrolment. We may ask the individual to specify the information their request relates to in order provide the information requested.

Section C: Right of rectification

6 The College will meet the right to rectification as follows:

- The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

- **An individual can make a request verbally or in writing.** Staff members receiving a request verbally will log the details of the request and forward the request to the Compliance Manger.

- **Details of the process for making a request including ID verification, timescales, fees and refusing requests are included at Appendix 2**

- Where the College receives a request for rectification, it will take reasonable steps to satisfy itself that the data is accurate and to rectify the data if necessary. The College will take into account the arguments and evidence provided by the data subject. The College may wish to check with the requester that it has understood the request, as this can help avoid later disputes about how the College has interpreted the request. The College will keep a log of verbal requests.

- What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort you should put into checking its accuracy and, if necessary, taking steps to rectify it. For example, we will make a greater effort to rectify inaccurate personal data if it is used to make significant decisions that will affect an individual or others, rather than trivial ones.

- We will also take into account any steps we have already taken to verify the accuracy of the data prior to the challenge by the data subject.

- The College may refuse a request and it is aware of the information we need to provide to individuals when we do so.

- Determining whether personal data is inaccurate can be more complex if the data refers to a mistake that has subsequently been resolved. It may be possible to argue that the record of the mistake is, in itself, accurate and should be kept. In such circumstances the fact that a mistake was made and the correct information should also be included in the individual's data. The GDPR does not give a definition of the term accuracy. However, the Data Protection Bill states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

- It is also complex if the data in question records an opinion. Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say

that it is inaccurate and needs to be rectified.

- An individual has the right to request restriction of the processing of their personal data where they contest its accuracy and the College is checking it. As a matter of good practice, the College will restrict the processing of the personal data in question whilst it is verifying accuracy, whether or not the individual has exercised their right to restriction.

- Where the College is satisfied that the data is accurate, we will let the individual know that we are satisfied that the personal data is accurate, and tell them that we will not be amending the data. The College will explain the decision, and inform the individual of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy.

- The circumstances in which the College may extend the time to respond may include further consideration of the accuracy of disputed data - although the College may only do this in complex cases - and the result may be that at the end of the extended time period you inform the individual that you consider the data in question to be accurate.

- If the College has disclosed the personal data to other organisations, we will contact each recipient and inform them of the rectification or completion of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, we will also inform the individual about these recipients.

- The GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Section D: Right to erasure

7 The College will meet the right to erasure as follows:

- Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

- Individuals have the right to have their personal data erased if:

    - the personal data is no longer necessary for the purpose which we originally collected or processed it for;
    - we are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;
    - we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
    - we are processing the personal data for direct marketing purposes and the individual objects to that processing;
    - we have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
    - we have to do it to comply with a legal obligation; or

    - we have processed the personal data to offer information society services to a child.

- There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the GDPR. Therefore, if we process data collected from children, we should give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet. This is still the case when the data subject is no longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent.

- **An individual can make a request verbally or in writing.** Staff members receiving a request verbally will log the details of the request and forward the request to the Compliance Manger.

- **Details of the process for making a request including ID verification, timescales, fees and refusing requests are included at Appendix 2.**

- The GDPR specifies two circumstances where we should tell other organisations about the erasure of personal data:

    - the personal data has been disclosed to others; or
    - the personal data has been made public in an online environment (for example on social networks, forums or websites).

- If the College has disclosed the personal data to others, we must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, we will also inform the individuals about these recipients.

- The GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

- Where personal data has been made public in an online environment reasonable steps should be taken to inform other controllers who are processing the personal data to erase links to, copies or replication of that data. When deciding what steps are reasonable you should take into account available technology and the cost of implementation.

- The right to erasure does not apply if processing is necessary for one of the following reasons:

    - to exercise the right of freedom of expression and information;
    - to comply with a legal obligation;
    - for the performance of a task carried out in the public interest or in the exercise of official authority;

- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

- The GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

    - if the processing is necessary for public health purposes in the public interest (eg protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
    - if the processing is necessary for the purposes of preventative or occupational medicine (eg where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).

- We will also provide this information if we request a reasonable fee or need additional information to identify the individual.

Section E: Right to restrict data

8 The College will meet the right to restrict data as follows:

- Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

- Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how you have processed their data. In most cases you will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time.

- Individuals have the right to request you restrict the processing of their personal data in the following circumstances:

    - the individual contests the accuracy of their personal data and you are verifying the accuracy of the data;
    - the data has been unlawfully processed (ie in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
    - you no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
    - the individual has objected to you processing their data under Article 21(1), and you are considering whether your legitimate grounds override those of the individual.

- The right to restrict data is distinct from the right to rectification and the right to object, there are close links between those rights and the right to restrict processing:

    - if an individual has challenged the accuracy of their data and asked for you to rectify it (Article 16), they also have a right to request you restrict processing while you consider their rectification request; or
    - if an individual exercises their right to object under Article 21(1), they also have a right to request you restrict processing while you consider their objection request.

- As a matter of good practice the College will automatically restrict the processing whilst it is considering its accuracy or the legitimate grounds for processing the personal data in question.

- **An individual can make a request verbally or in writing.** Staff members receiving a request verbally will log the details of the request and forward the request to the Compliance Manger.

- **Details of the process for making a request including ID verification, timescales, fees and refusing requests are included at Appendix 2.**

- The College will take action to restrict personal data if required. It is important to note that the definition of processing includes a broad range of operations including collection, structuring, dissemination and erasure of data. Therefore, we will use methods of restriction that are appropriate for the type of processing we are carrying out.

- The GDPR suggests a number of different methods that could be used to restrict data, such as:

    - temporarily moving the data to another processing system;
    - making the data unavailable to users; or
    - temporarily removing published data from a website.

- The College will consider how it stores personal data that is no longer needed to process but the individual has requested is restricted (effectively requesting that the College does not erase the data).

- Where we are using an automated filing system, we will use technical measures to ensure that any further processing cannot take place and that the data cannot be changed whilst the restriction is in place. We will also note on your system that the processing of this data has been restricted.

- The College will not process the restricted data in any way **except to store it** unless:

    - we have the individual's consent;
    - it is for the establishment, exercise or defence of legal claims;
    - it is for the protection of the rights of another person (natural or legal); or
    - it is for reasons of important public interest.

- If the College has disclosed the personal data in question to others, we will contact each recipient and inform them of the restriction of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, the College will also inform the individual about these recipients.

- In many cases the restriction of processing is only temporary, specifically when the restriction is on the grounds that:

    - the individual has disputed the accuracy of the personal data and you are investigating this; or
    - the individual has objected to you processing their data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of your legitimate interests, and you are considering whether your legitimate grounds override those of the individual.

- Once the College has made a decision on the accuracy of the data, or whether your legitimate grounds override those of the individual, you may decide to lift the restriction.

- If we do this, the College will inform the individual **before** you lift the restriction. As noted above, these two conditions are linked to the right to rectification (Article 16) and the right to object (Article 21). This means that where the College is informing the individual that you are lifting the restriction (on the grounds that you are satisfied that the data is accurate, or that our legitimate grounds override theirs) we will also inform them of the reasons for our refusal to act upon their rights under Articles 16 or 21. The College will also inform the individual of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek a judicial remedy.

Section F: Right to data portability

9 The College will meet the right to data portability as follows:

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

- Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe.

- It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

- The right to data portability only applies:

    - to personal data an individual has provided to a controller;
    - where the processing is based on the individual's consent or for the performance of a contract; and
    - when processing is carried out by automated means.

- The College will provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

- The information will be provided free of charge.

- If the individual requests it, we may transmit the data directly to another organisation if this is technically feasible. However, the College is not required to adopt or maintain processing systems that are technically compatible with other organisations.

- If the personal data concerns more than one individual, the College will consider whether providing the information would prejudice the rights of any other individual.

- The College will respond without undue delay, and within one month. This may be extended by two months where the request is complex or the College receives a number of requests. We will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

- Where the College is not taking action in response to a request, we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Section G: Right to object

10 The College will meet the right to object as follows:

- Individuals have the right to object to:

    - processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
    - direct marketing (including profiling); and
    - processing for purposes of scientific/historical research and statistics.

- Individuals must have an objection on “grounds relating to his or her particular situation”.

- The College will stop processing the personal data unless:

    - it can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
    - the processing is for the establishment, exercise or defence of legal claims.

- We inform individuals of their right to object “at the point of first communication” which is the College Enrolment Form and in the **STCG Privacy Notice**.

- This right will be “explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information”.

- The College will stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.

- We will deal with an objection to processing for direct marketing at any time and free of charge.

- Individuals must have “grounds relating to his or her particular situation” in order to exercise their right to object to processing for research purposes.

- Where the College is conducting research where the processing of personal data is necessary for the performance of a public interest task, we may not comply with an objection to the processing.

- The College will provide way for individuals to object online through its website.

Section H: Rights related to automated decision making

11 The College will meet the rights related to automated decision making as follows:

- The GDPR has provisions on automated individual decision-making (making a decision solely by automated means without any human involvement); and

- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

- The GDPR applies to all automated individual decision-making and profiling. Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.

- The College will only carry out this type of decision-making where the decision is:

    - necessary for the entry into or performance of a contract; or
    - authorised by Union or Member state law applicable to the controller; or
    - based on the individual's explicit consent.

- **The College does not undertake processing that falls under the category of automated decision making.**

Section I: Contracts

12 The College will meet the requirements for contracts as follows:

- The GDPR makes written contracts between controllers and processors a general requirement, rather than just a way of demonstrating compliance with the seventh data protection principle (appropriate security measures) under the DPA.

- The GDPR allows for standard contractual clauses from the EU Commission or a supervisory authority (such as the ICO) to be used in contracts between controllers and processors. No standard contractual clauses have been issued by the EU or ICO. The College has been provided with its own legal advice on standard clauses.

- The GDPR envisages that adherence by a processor to an approved code of conduct or certification scheme may be used to help controllers demonstrate that they have chosen a suitable processor. Standard contractual clauses may form part of such a code or scheme, though again, no schemes are currently available.

- The GDPR gives processors responsibilities and liabilities in their own right, and processors as well as controllers may now be liable to pay damages or be subject to fines or other penalties.

- Whenever a controller uses a processor (a third party who processes personal data on behalf of the controller) it needs to have a written contract in place. Similarly, if a processor employs another processor it needs to have a written contract in place. Contracts between controllers and processors ensure that they both understand their obligations, responsibilities and liabilities. They help them to comply with the GDPR, and help controllers to demonstrate their compliance with the GDPR. The use of contracts by controllers and processors may also increase data subjects' confidence in the handling of their personal data.

- Contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller.

- **The College will identify all contracts where it is either the controller or processor. The Compliance Manager will retain a log of these contracts and their nature. The College will maintain a Contracts Log.**

- Where the College is the **data controller**, it will ensure that contracts will include as a minimum the following terms, requiring the **processor** to:

    - only act on the written instructions of the controller;
    - ensure that people processing the data are subject to a duty of confidence;
    - take appropriate measures to ensure the security of processing;
    - only engage sub-processors with the prior consent of the controller and under a written contract;
    - assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
    - assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
    - delete or return all personal data to the controller as requested at the end of the contract; and

- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

- A processor must only act on the documented instructions of a controller. If a processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a controller and will have the same liability as a controller.

- Where the College is the **data processor**, it will ensure that it meets contractual obligations to the controller, under the GDPR a processor also has the following direct responsibilities:

    - not to use a sub-processor without the prior written authorisation of the data controller;
    - to co-operate with supervisory authorities (such as the ICO);
    - to ensure the security of its processing;
    - to keep records of processing activities;
    - to notify any personal data breaches to the data controller;
    - to employ a data protection officer; and
    - to appoint (in writing) a representative within the European Union if needed.

- If a processor fails to meet any of these obligations, or acts outside or against the instructions of the controller, then it may be liable to pay damages in legal proceedings, or be subject to fines or other penalties or corrective measures.

- If a processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor's obligations.

Section J: Documentation – Information Asset Register

12 The College will meet the requirements for documentation as follows:

- The documentation of processing activities is a new requirement under the GDPR.

- We are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention; we call this **documentation**.

- By documenting our processing activities, we are able to meet a legal requirement, but also support good data governance and demonstrate compliance with other aspects of the GDPR.

- Controllers and processors each have their own documentation obligations. As the College has 250 or more employees, it will document all processing activities.

- **The College will maintain an Information Asset Register which is the documentation log.**

Section K: Data Sharing with Local Authorities

14 Under the Education and Skills Act 2008, Local Authorities have a duty to track participation of all 16 to 17 year olds resident in their area, and to make arrangements for those not in education or training. In some cases, the Local Authority commission a 3rd party to help fulfil their duties on their behalf.

15 The College is required to share data with each home Local Authority in order for them to fulfil these duties, if an individual falls into one or more of the following categories:

- 16 to 17 years of age
- a vulnerable adult in care of the Local Authority or previously in care of the Local Authority
- 18-24 years old with an Education Health Care Plan (EHCP).

16 The Data Sharing Agreement is set out at Appendix 3.

Section L: Data Protection Impact Assessments

17 The College will meet the requirements for the Data Protection Impact Assessment (DPIA) requirement as follows:

- A DPIA is a process to systematically analyse the College processing and help it identify and minimise data protection risks. We will:
    - describe the processing and the purposes;
    - assess necessity and proportionality;
    - identify and assess risks to individuals; and
    - identify any measures to mitigate those risks and protect the data.
- The College does not expect to eradicate the risk, but the process should help to minimise risks and consider whether or not they are justified.
- The College will complete a DPIA for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability more generally and building trust and engagement with individuals.
- A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.
- **The College will include DPIA as part of its Corporate Risk Management Process. The Risk Register will include any data processing risk that are considered to be 'High Risk'. These risk will be reported through the Risk Management and Board Assurance Process.**
- DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or

economic disadvantage. The focus is on the potential for harm – whether physical, material or non-material - to individuals or to society at large.

- To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It should look at risk based on the specific nature, scope, context and purposes of the processing.

- We will conduct a DPIA before we begin any type of processing which is "likely to result in a high risk". This means that although the actual level of risk has not been assessed yet, we will screen for factors which point to the potential for a widespread or serious impact on individuals.

- In particular, the GDPR indicated that the College will do a DPIA if it plans to:

    - use systematic and extensive profiling with significant effects;
    - process special category or criminal offence data on a large scale; or
    - systematically monitor publicly accessible places on a large scale.

- The ICO also requires the College to do a DPIA where we plan to:

    - use new technologies;
    - use profiling or special category data to decide on access to services;
    - profile individuals on a large scale;
    - process biometric data;
    - process genetic data;
    - match data or combine datasets from different sources;
    - collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
    - track individuals' location or behaviour;
    - profile children or target services at them; or
    - process data that might endanger the individual's physical health or safety in the event of a security breach.

- The College will also consider doing a DPIA for any other processing which is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

Section M: Data Breach Policy

18 The College will meet the requirements for the managing Data Breach as follows:

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority, the Information Commissioners Office (ICO), within 72 hours of becoming aware of the breach, where feasible.

- Recital 87 of the GDPR makes clear that when a security incident takes place, South Thames College Group (STCG) should quickly establish whether a personal data

breach has occurred and, if so, promptly take steps to address it.

- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, STCG must also inform those individuals without undue delay.

- STCG have a legal duty to keep a record of any personal data breaches, regardless of whether we are required to notify.

Personal data

- A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

- Personal data is defined as:

  ''*data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller."*

- Where a personal data breach has occurred STCG will assess the likelihood and severity of the resulting risk to people's rights and freedoms. This will include consideration of whether this breach will result in result in:

  "physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

Reporting a breach

- All personal data breaches, whether suspected or confirmed, must be reported by the member of staff to the group Data Protection Officer (DPO) without delay.

- Staff must follow the following three steps:

  - **Step one: Report the breach to the DPO -** Data breaches should be reported via telephone; to ensure any required action can be taken at the earliest opportunity.

  - **Step Two: Send a breach notification report to the DPO** - a summary email must be sent within one hour of the call.

  - The email will be referred to as the 'breach notification report'. The breach notification report must include (as a minimum):

    - date and time of the breach (if known)
    - who reported the breach, if different to the person sending the email
    - nature of the breach e.g. theft, loss or damage
    - a description of the personal data involved (without identifiers)
    - the type and number of persons impacted e.g. 10 students

        - any corrective action(s) taken

    - **Step Three: Take no further action** - Once the breach is reported, no further action should be taken by the staff member unless they are requested to do so by the DPO. The DPO will assume responsibility from this point forward.

Data Breach Investigation form (DPO)

- The Data Breach Investigation form must be completed by the DPO, or a nominated Data Protection specialist.

- The purpose of the Investigation form is to document the circumstances of the breach, what actions have been taken and what recommendations have been made.

- The objective of any breach investigation is to identify what actions the organisation needs to take to alleviate any risks to individuals, to prevent a recurrence of the incident and to determine whether the incident needs to be reported to the ICO.

- In all cases the DPO will act as the point of contact for the ICO.

- **Appendix 4 provides a copy of the Data Breach Form.**

Appendix 1 – STCG Privacy Notice (students and other stakeholders)

Introduction

South Thames Colleges Group (the College) is required to collect personal data from its customers. South Thames Colleges Group includes Carshalton College, Kingston College, Merton College and South Thames College.

This privacy notice details how we collect your data, what we use it for, what actions you can take if you wish to access your data and how to make changes to the way we are using it.

How we use your data

The data you provide us will only be used by the College for purposes relating to:

- your education and training
- employment
- advice and well-being
- marketing and research

You will be asked to provide personal information about yourself in order to enquire, apply and / or enrol to one of our courses or access our services.

At the point of collecting this data we always aim to clearly explain what it is going to be used for and who we may share it with.

Unless required or permitted by law, we will always ask you before we use it for any other reason. We would only use it for marketing with your prior consent.

Any sensitive personal information will never be supplied to anyone outside the College without first obtaining your consent, unless required or permitted by law.

The basis for collecting data and your rights

Most of the data we collect from you is essential for your enrolment as a student in order to access funding, or is required by law. You must provide the data in order to enrol with us and we will make this clear at time of enrolment.

Other data is collected on your consent, and you may withdraw this consent without this affecting your status as a student.

You have a variety of rights about the way we process your data:

- You can request a copy of the data we hold about you
- You may change or stop the way in which we communicate with you
- You may change or stop us processing data about you, if it is not required for the purpose you originally provided it
- If you are not satisfied with the way we have processed your data, then you can complain to the Office of the Information Commissioner (ICO)

More information about your rights can be found on the ICO website here https://ico.org.uk/

Government and funding Agencies

We are required to share your data with certain Government and funding agencies in order to meet our contractual and legal obligations, specifically the Education and Skills Funding Agency (ESFA) and the Office for Students (OFS).

The ESFA will share your data with the Department for Education (DfE) and the European Social Fund (ESF) Managing Authority.

Further information can be found here:

ESFA https://www.gov.uk/government/publications/esfa-privacy-notice

OFS https://www.officeforstudents.org.uk/privacy/

Local Authorities

Under the Education and Skills Act 2008, Local Authorities have a duty to track participation of all 16 to 17 year olds resident in their area, and to make arrangements for those not in education or training. In some cases, the Local Authority commission a 3rd party to help fulfil their duties on their behalf.

The College is required to share your data with your Local Authority in order for them to fulfil these duties, if you fall into one or more of the following categories:

- 16 to 17 years of age
- a vulnerable adult in care of the Local Authority or previously in care of the Local Authority
- 18-24 years old with an Education Health Care Plan (EHCP).

How long do we keep your data

We will keep your data for as long as is needed to complete the task for which it was collected. The College Data Retention Policy sets out the specific retention periods for your personal data and this can be found on the College website.

How we keep your data safe

The College takes data security very seriously and has a number of robust systems in place to keep your information secure.

These include a range of physical, technical and organisational security measures, such as access control, an encrypted network and secure storage.

The College has a number of internal policies of which staff and our partners are required to follow, with training and awareness-raising activities undertaken to promote compliance with data protection legislation.

Data protection procedures are regularly reviewed and the College maintains an Information Asset Register of all key personal data; its business purpose, location and how it is secured.

Contact us

If you have any questions about this privacy statement or how we communicate with you, please contact:

South Thames Colleges Group
Kingston Hall Road
Kingston Upon Thames
KT1 2AQ
Tel. 020 8918 7777

You can also email us at:

Carshalton College **-** feedback@carshalton.ac.uk

Kingston College - feedback@kingston-college.ac.uk

South Thames College - feedback@south-thames.ac.uk

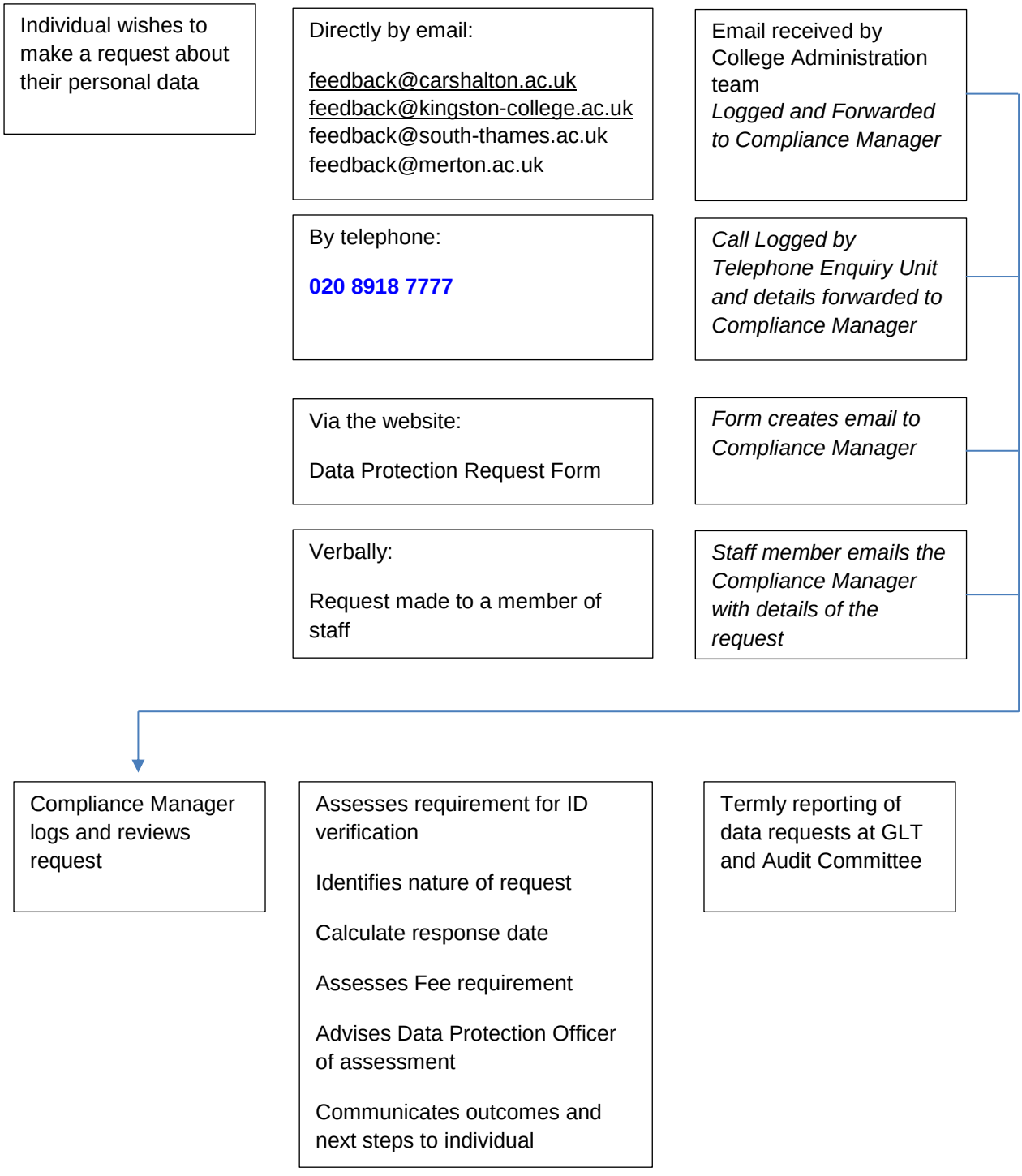
Merton College - feedback@merton.ac.uk

Data Protection Registration Number: **Z7473315**

Data Protection Officer(s):

Chris Wright **Deputy CEO** **Data Protection related to:** **Finance, HR and Estates**	**Robin Greenaway** **Deputy CEO** **Data Protection related to:** **Curriculum & Quality, Data & Systems**

Appendix 2 – Process for handling Individual Rights requests



Appendix 2 – Process for handling Individual Rights requests (continued)

ID verification

- Where the College has doubts about the identity of the person making a request we may ask for more information. However, we will only request information that is necessary to confirm the identity of the requester. We will take into account what data we hold, the nature of the data, and what we are using it for.

- We will let the individual know without undue delay and within one month that we need more information from them to confirm their identity. We may not comply with the request until the College has received the additional information.

Timescale for response

- The College will respond to a request without undue delay and within one month of receipt. We will calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

- This may be extended by two months where the request is complex or the College receives a number of requests. We will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Fees and refusing requests

- Generally the College will not charge a fee for processing requests.

- If the College considers that a request is manifestly unfounded or excessive we may:

    - request a "reasonable fee" to deal with the request; or
    - refuse to deal with the request.

- We will base the fee on the administrative costs of complying with the request. If we decide to charge a fee we will contact the individual promptly and inform them. We may not comply with the request until the College has received the fee.

- Where the College refuses to respond to a request, it will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

- we will inform the individual without undue delay and within one month of receipt of the request about:

    - the reasons the College is not taking action including where we request a reasonable fee or need additional information to identify the individual;
    - their right to make a complaint to the ICO or another supervisory authority; and
    - their ability to seek to enforce this right through a judicial remedy.

Appendix 3 – Data Sharing Agreement for Local Authorities

THIS DATA SHARING AGREEMENT is made on the ENTER DATE HERE

BETWEEN

(1) South Thames Colleges Group**, Kingston Hall Rd Kingston upon Thames, Surrey KT1 2AQ, United Kingdom**. ("the College").

(2) [Company Name], [Company Number]) whose registered office address is [Registered Office] ("the Partner").

PURPOSE

A Data Sharing Agreement must be completed where data is routinely shared between the College and the Partner. It must cover the types of data that will be shared and how this will be done securely, in accordance with Data Protection legislation.

The original must be retained by the issuing College Director with a copy submitted to the College Data Protection Officer for central record. Where any changes are required a new copy of the agreement must be completed.

RESPONSIBILITIES

The College:

- owns and is responsible for the content of the personal data set out in schedule one
- authorises the Partner to process the personal data for the purposes set out in schedule one
- specifies the duration to which the personal data can be used
- specifies the agreed methods for transferring and storing the personal data

The Partner:

- must ensure that Data Protection Principles are upheld, in accordance with Data Protection legislation
- provide the details of the representatives processing the personal data
- Ensure that all information exchanged is kept secure, confidential and up to date
- Dispose of the personal data securely once the Sharing Agreement comes to an end, or when it is no longer legally or contractually required
- Report any data breaches to the College within 24 hours of the breach
- Maintain an audit trial of all activity and allow the College access to audit procedures, storage and destruction arrangements as required

SCHEDULE ONE: PERSONAL DATA SHARE

Section one: to be completed by the College representative

Subject matter of Processing	[Personal data relating to a learner *or learners* progress on their course]
Duration of Processing	[1st August 2017 – 31st July 2018]
Purpose of Processing	[Educational]
Type of Personal Data	[Name, DOB, contact details, attendance, course progress, relevant safeguarding records]
Categories of Data Subject	[Enrolled learners (contracted)]
Basis for Processing	[Article 6(1)(a) Consent; Article 6(1)(c) - legal obligation; Article 6(1)(b) Contract; Article 9(2)(b) - social protection]
Method(s) of Data Share	[ProPortal access; secure email (password protected)]

Section two: to be completed by the Partner representative

Named Data Processors	
Named Data Protection Officer	
Method(s) for securely storing the data	
Location of the data storage	
Date of destruction / retention date *if different to the processing end date in section one. Specify the contractual or legal basis for retaining the data for this period.*	

STATEMENT

By signing below, we confirm that the arrangements described above accurately represent the data shared and the methods and formats of transfer as well as and other recordkeeping arrangements required.

Where personal data is being shared, we also confirm that the information will be used only for the purposes stated only in this agreement and will not be shared with or passed to any third parties not already named in this agreement. When personal data is disposed of this will be done in such a way to ensure confidentiality is preserved.

Where personal data is being collected in order to be shared, data subjects have been informed and given consent where required to do so.

SIGNED FOR AND ON BEHALF OF

Partner

Name……..…….…… Position ……..…….……

Signature…… Date …/…/……

College

Name……..…….…… Position ……..…….……

Signature……..… Date …/…/……

Appendix 4 – Data Breach Investigation Form

Carshalton College | Kingston College | Merton College | South Thames College

SOUTH THAMES COLLEGES GROUP

This investigation form must be completed within 48 hours, in order for STCG to meet its reporting obligations. Where this is not possible, the form must be completed at the earliest opportunity.

Data Breach Investigation form

Name	
Job title	
Role e.g. DPO	
Date	

1. Summary	
Date and time of Incident	
How you became aware of the breach (specify date, time and who reported it)	
Nature of breach e.g. disclosed in error / technical problem / theft	
Description of how breach occurred	
Full description of personal data involved (without identifiers)	

Number of people whose data is affected	
2. Impact	
Describe the risk of harm to the individual(s) as a result of this incident	
Describe the risk of identity theft as a result of this incident	
Have you received a formal complaint from any individual affected by this breach? If so, provide details	
3. Action(s) taken	
What immediate remedial action was taken. Has the data been retrieved or deleted? If yes - date and time	
Have all affected individuals been informed? If not, state why not	
Is there any evidence to date that the personal data involved in this incident has been inappropriately processed or further disclosed? If so, please provide details	
4. Management	

Do you consider the employee(s) involved has broken policy and / or procedures	
Do you consider whether any other personal data held may be exposed to similar vulnerabilities? If so, what steps have been	
Has there been any media coverage of the incident? If so, please provide details	
What further action has been taken to minimise the possibility of a repeat of such an incident e.g. review of systems, further training	
Please inform of any disciplinary action taken in relation to the employee(s) involved:	

ACTION PLAN	**Yes**	**No**	**Not required**
Individuals contacted	Enter date	Enter date	Enter date
ICO contacted	Enter date	Enter date	Enter date
Human resources notified	Enter date	Enter date	Enter date
Breach logged with Audit Committee	Enter date		

Signed	
Date	

Appendix 5 – STCG Privacy Notice (Staff)

Privacy Notice – Personal information about Staff, Applicants and Governors

Introduction

At South Thames Colleges Group (the Group), we are committed to protecting and respecting your privacy. This notice deals specifically with employees and applicants and is part of the General Data Protection Regulations (GPDR) policy and procedures for the Group. In the case of governors, this notice also applies to their personal information where it is collected by the Group.

The Group collects and processes personal data relating to its employees and applicants to manage the employment relationship and recruitment process. We are committed to being transparent about how we collect and use that data and to meeting our data protection obligations.

This notice explains when and why we collect personal information about employees and applicants, how we use it and the conditions under which we may disclose it to others, how we keep it secure and your rights in relation to that data.

We may change this notice, if for example there is a change in legislation or a change in our data processing. Should this occur we will notify all employees and make future applicants aware of this.

What information do we hold about you and your employment?

On commencement of your employment, we will ask you to provide certain personal information about yourself to enable us to ensure that we can communicate with you, ensure that you are paid and to hold data required of us by legislation. This data is also necessary in order for the group to meet its obligations under your employment contract. This will include information such as your home address, bank details, Next of Kin, National Insurance number, Ethnicity and other equality information, salary and pension information.

How do we collect information from you?

We obtain information from you through a variety of methods and depending on whether you are an employee or recruitment candidate.

Employees: We obtain information from your original recruitment application form that is then transferred to your employee record. Throughout your employment at the college we will collect data about you from a variety of sources, such as appraisals completed, absence information from self-certificates and fit notes, changes to your employment such as a reduction in hours or a promotion.

Recruitment Candidates: We collect directly from you the information that you provide on your application form. Other information on you may be obtained from third parties such as references, occupational health clearance and disclosure and barring certificate (DBS) if you are successful at interview.

What information do we collect from you?

The personal information we collect about you includes but is not limited to:

Personal details – name, date of birth, address

Qualifications – we record on the HR system and your file the qualifications that you have provided to us

Health details – we hold sick certificates should you have been absent from work and may also hold medical reports from your GP or Occupational health.

Equality data – we record this data to ensure that we complying with the Equality Act 2010 in offering reasonable adjustments were required and in monitoring our equality data to ensure there is no discrimination.

Financial information – this will include your current and historical remuneration as well as your bank details and any benefits you may be entitled to for example, pension, childcare vouchers.

What information do we share with third parties and why?

We share certain details relating to your employment or application for employment with identified third parties to enable us to process your data for legal and organisational reasons. These include:

Cascade and iTrent – these are the managed HR systems that the College uses to hold employees records.

Pensions – certain basic data is shared with the pension scheme relevant to your employment with the College, to satisfy the requirements of auto-enrolment and pensions regulations.

HMRC – Information is provided so that your tax and national insurance payments are correct.

DBS/E-Safeguarding – This is in order to fulfil our obligations under 'Keeping Children safe in education' whereby a DBS is required for new employees and also the Further Education Regulations (England) 2006. Information such as your personal details, passport details, address details are provided to E-Safeguarding in order for them to provide a DBS check for you.

Midland payroll – information such as bank details, current remuneration and any changes to your pay are provided for South Thames College and Merton College employees.

Occupational Health – Information is provided to occupational health providers such as personal details, contact details and ill health information. This is so that occupational health can provide informed advice concerning an employee's wellbeing and to recommend actions to support an employee during their period of absence and on their return to work.

Who has access to your information?

We will only share data internally to those that require this information and where this is necessary. This includes the HR Team, Payroll, your manager and senior managers of the college, as well as the recruitment team involved in the recruitment process.

We will not sell or rent your information to third parties.

We only share the above information with third parties where it is a requirement. We ensure that these providers protect your data by committing to only processing your data on our behalf and processing it in line with the General Data Protection Regulations.

Data we provide to other third parties, such as responses to requests under the Freedom of Information Act and compliance with our duty under the Single Quality Scheme, is anonymised so that individual staff cannot be identified.

Requests for information relating to your employment, which are not required by law, are responded to where explicit permission has been provided by yourself.

There are some situations where your information can be shared for other reasons, such as to prevent a crime or a request from the Police for your details to assist in an investigation.

How you can access and update your information?

The accuracy of your information is important to us. You can request to see your file so that you can check the contents of this and we ask that you provide at least one weeks notice.

The HR system, Cascade for employees at Kingston and Carshalton and iTrent at South Thames College and Merton, contains the details we hold for you and you can view these online and either change them online, if you are using cascade or request for them to be changed through the HR team if you are using iTrent. Access to the HR system is password protected to each employee.

Your rights

You have a variety of rights about the way we process your data as an employee or applicant to the Group:

- You can request a copy of the data we hold about you
- You may change or stop the way in which we communicate with you
- You may change or stop us processing data about you, if it is not required for the purpose you originally provided it

If you are not satisfied with the way we have processed your data, then you can complain to the Office of the Information Commissioner (ICO)

Please note that you have some obligations under your contract of employment to provide us with data. In particular, for example, you are required to report absence from work and provide us

with information in order to exercise your statutory rights and failing to provide this may mean you are unable to exercise your statutory rights.

Contact us

If you have any queries regarding this policy or data processing within the HR department please contact the relevant HR team, or alternatively you can contact the Groups nominated data protection officer(s):

Chris Wright **Deputy CEO** **Data Protection related to:** **Finance, HR and Estates**	**Robin Greenaway** **Deputy CEO** **Data Protection related to:** **Curriculum & Quality, Data & Systems**

Other Relevant Policies:

Group Data Protection Policy

Appendix 6 – Data Retention Policy

1 INTRODUCTION

1.1 South Thames Colleges Group (the "**College**") must, in respect of its processing of personal data, comply with the Data Protection Act 2018, the General Data Protection Regulation 2016/679, and related legislation (together, "**Data Protection Laws**").

1.2 This Retention Policy should be read in conjunction with the College's GDPR Policy, which sets out the College's overall approach to data protection matters.

1.3 The College is under a legal obligation only to keep personal data for as long as the College needs it. Once the College no longer needs personal data, the College must securely delete it. The College recognises that the correct and lawful treatment of data will maintain confidence in the College and will provide for a successful working environment.

1.4 This Policy applies to all College employees, consultants, contractors and temporary personnel hired to work on behalf of the College ("**College Personnel**").

1.5 All College Personnel with access to personal data must comply with this Retention Policy.

1.6 Please read this Retention Policy carefully. All College Personnel must comply with it at all times. If you have any queries regarding this Retention Policy, please consult your manager and/ or the Data Protection Officer. You are advised that any breach of this Retention Policy will be treated seriously and may result in disciplinary action being taken against you.

1.7 College Personnel will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any College Personnel's contract of employment and the College reserves the right to change this Policy at any time. All College Personnel are obliged to comply with this Policy at all times.

2 ABOUT THIS POLICY

2.1 This Retention Policy explains how the College complies with our legal obligation not to keep personal data for longer than we need it and sets out when different types of personal data will be deleted. In particular, it sets out details of the College's policies for the retention of Special Category personal data.

3 DATA RETENTION PERIODS

3.1 The College has assessed the types of personal data that the College holds and the purposes the College use it for. The table below sets out the retention periods that the College has set for the different departments within the College, and the different types of data that they each hold.

3.2 If any member of College Personnel considers that a particular piece of personal data needs to be kept for more or less time than the period set out in this policy, please contact the Data Protection Officer for guidance.

3.3 All paper records will be securely destroyed at the date of deletion and all electronic files will be deleted at the date of deletion.

4 RETENTION PERIODS FOR DIFFERENT CATEGORIES OF DATA

Record	**When will the College delete it (paper)?**	**When will the College delete it (if electronic)**
Students		
Application Form	Current + 1 year	Current + 5 years
Learning Agreement & Student Files (Non-ESF)	Current + 2 years	
Learning Agreement & Student Files (ESF)	At 31 Dec 2030	
Enrolment and Achievement Records (Non-ESF)		Current + 10 years
Enrolment and Achievement Records (ESF)		At 31 Dec 2030
Attendance Registers	Current + 2 years	
Attendance Record		Current + 10 years
Examination Entries (Non-ESF)	Current + 6 years (or Awarding Body requirement)	
Examination Entries (ESF)	At 31 Dec 2030	
Examination Results (Non-ESF)	Current + 6 years (or Awarding Body requirement)	
Examination Results (ESF)	At 31 Dec 2030	
Unclaimed Examination Certificates	Current + 6 years (or Awarding Body requirements)	
Tutorial Files and Student Tracking (Non-ESF)	Current + 2 years	Current + 2 years
Tutorial Files and Student Tracking (ESF)	At 31 Dec 2030	At 31 Dec 2030
General Correspondence & Subject Files	Current + 1 year	
Payment Records	Current + 6 years	Current + 6 years
Cash Receipts	Current + 6 years	
Staffing records		
Personnel files	Current + 6 years from the end of employment	Current + 6 years from the end of employment

Application forms/interview notes	Current + 1 year from the date of the interviews	Current + 1 year from the date of the interviews
Income Tax and NI returns	Current + 6 years	Current + 6 years
Statutory Maternity Pay records	Current + 6 years	Current + 6 years
Statutory Sick Pay records and	Current + 6 years	Current + 6 years
Wage and salary records	Current + 6 years	Current + 6 years
Accident books and records	Current + 13 years after the date of incident	
Health records where reason for termination of employment is health related.	Current + 3 years	
Health & Safety Records	10 Years	
Medical Records kept by reason of COSHH	40 years	

5 CHANGES TO THIS POLICY

The College reserves the right to change this policy at any time.