South Staffordshire College

Data Protection Policy

Reference: Version	Final
Policy Originator:	Deputy Principal Finance & Resources
Equality Impact Assessed:	September 2024
Approved by:	Board
Date Approved:	October 2024
Review Interval:	Biennial
Last Review Date:	November 2022
Next Review Date:	October 2026
Audience:	All Staff and Governors

1.0 Policy Statement

1.1 The purpose of this policy is to establish the approach of the College to data protection and the requirements of the Data Protection Act 2018.

1.2 Personal data is data relating to a living individual who can be identified from it alone, or when it is combined with other information held by the College or which the College is likely to receive. This can include sensitive (special category) data relating to an individual's gender, age, ethnicity, disability, trade union membership, political opinions, religious or similar beliefs, physical or mental health, sexual life, or information relating to criminal proceedings or outcomes.

1.3 The College has a procedure for processing special category and criminal conviction data specifically, in line with the Data Protection Act (DPA) 2018.

1.4 This data can be held electronically, or in structured manual records or even in some cases in unstructured manual records. It can also refer to information held as images or a video recording such as CCTV images.

1.5 As an organisation that obtains, views, uses, discloses, destroys and stores Personal Data about its employees, suppliers (sole traders, partnerships or individuals within companies), students, alumni, governors, parents and visitors and commercial customers, the College recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with the College's obligations under Data Protection Laws and in particular its obligations under Article 5 of UK GDPR.

1.6 The College has implemented this Data Protection Policy to ensure all College Staff are aware of what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in the College and maintain its reputation and will provide for a successful working and learning environments for all.

1.7 College staff will be referred to this Policy when joining as a new member of staff. This Policy does not form part of any member of the College staff's contract of employment and the College reserves the right to change this Policy at any time. All members of College staff are obliged to comply with this Policy at all times.

1.8 GDPR is part of the College's mandatory CPD training suite of courses. Compliance with the training will be monitored to ensure that all staff complete the training on a periodic basis.

1.9 The following Policies and guidance are relevant to personal information:

- Social Media Guidelines
- Freedom of Information Policy

- Information Security Policy
- Data Breach Management Procedure
- Data Retention and Disposal Policy
- Data Subject Access Request Procedure (Annex 1)
- Procedure for processing special category and criminal conviction data
- Data Privacy Impact Assessment
- Disciplinary Procedures for staff and students
- Equality, Diversity and Inclusion (EDI) Policy
- Safeguarding Policy

1.10 The College will adhere to its obligations under other legislation relevant to the use of personal data, which include:

- Data Protection Act 2018 and UK General Data Protection Regulation
- Privacy and Electronic Communications Regulations 2003
- the Communications Act 2003
- the Human Rights Act 1998
- the Defamation Act 2013
- the Equality Act 2010
- the Safeguarding Vulnerable Groups Act 2006.

2.0 Scope

2.1 This Policy (and the other policies and documents referred to in it) sets out the basis on which the College will collect and use Personal Data either where the College collects it from individuals itself, or where it is provided to the College by third parties. It also sets out rules on how the College handles, uses, transfers, destroys and stores Personal Data.

2.2 The College collects data on its learners, employees, contractors, volunteers and associates for the following reasons:

- For financial and staffing records including salary and benefits, holiday and sickness, performance and achievement
- For safeguarding and other statutory obligations relating to staff and students such as equality, diversity and inclusion and health and safety
- To provide education and support to learners and promotion of these services
- To complete funding claims and contractual obligations
- To maintain of the security of the premises and for the prevention or detection of crime (including CCTV)

2.3 This is not an exhaustive list. More information on processing of data subjects' information is provided in the College's Privacy Notices for students, staff and other groups.

2.4 The Data Protection and Digital Information Bill was to be introduced but was halted by the July 2024 election. The Bill would have brought changes to the current legislation including:

- Removal of the requirement for a Record of Processing Activities;
- Removal of the requirement for a Data Protection Risk Assessment;
- Removal of the requirement for a Data Protection Officer,
- Other changes that were generally seen as reducing the onus on organisations.

3.0 Responsibilities

3.1 All College Staff, volunteers and governors must comply with this policy.

3.2 College Staff must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.

3.3 College Staff must not release or disclose any Personal Data by any means either outside of the College or within the College to staff not authorised to access the Personal Data unless they have specific authorisation from their manager or the Data Protection Officer.

3.4 College Staff must take all steps to ensure there is no unauthorised access to Personal Data whether by other College Staff who are not authorised to see such Personal Data or by people outside the College.

3.5 Any unauthorised disclosure of personal data to a third party by any staff member may result in disciplinary or legal action. Failure to comply with College policies and procedures for handling staff/student data is a disciplinary offence which may be considered gross misconduct and may also involve personal criminal liability.

4.0 Data Protection Principles

4.1 When using Personal Data, Data Protection Laws require that the College complies with the following principles. These principles require Personal Data to be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
- Accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;
- Kept for no longer than is necessary for the purposes for which it is being processed; and
- Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4.2 These principles are considered in more detail in the remainder of this Policy.

4.3 In addition to complying with the above requirements the College also has to demonstrate in

writing that it complies with them. The College has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the College can demonstrate its compliance.

5.0 Lawful Use and processing of Personal Data

5.1 In order to collect and/or use Personal Data lawfully the College needs to be able to show that its use meets one of a number of legal grounds. Please click here to see the detailed grounds https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing

5.2 In addition when the College collects and/or uses Special Categories of Personal Data, the College has to show that one of a number of additional conditions is met. Please click here to see the detailed additional conditions https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/special-category-data

5.3 The College has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 5.1 and 5.2. If the College changes how it uses Personal Data, the College needs to update this record and may also need to notify Individuals about the change. If College Staff therefore intend to change how they use Personal Data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

6.0 Transparent Processing – Privacy Notices

6.1 Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses their Personal Data via a privacy notice.

6.2 If the College receives Personal Data about an Individual from other sources, the College will provide the Individual with a privacy notice about how the College will use their Personal Data. This will be provided as soon as reasonably possible and in any event within one month.

6.3 If the College changes how it uses Personal Data, the College may need to notify Individuals about the change. If College Staff therefore intend to change how they use Personal Data please notify the Data Protection Officer who will decide whether the College Staff's intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

7.0 Data Quality – Ensuring the Use of Accurate, Up To Date and Relevant Personal Data

7.1 Data Protection Laws require that the College only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the Individual in a privacy notice (see paragraph 6 above) and as set out in the College's record of how it uses Personal Data. The College is also required to ensure that the Personal Data the College holds is accurate and kept up to date.

7.2 Accuracy and Relevance of Personal Data

All College Staff that collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

7.3 All College Staff that obtain Personal Data from sources outside the College shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require College Staff to independently check the Personal Data obtained.

7.4 In order to maintain the quality of Personal Data, all College Staff that access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to Personal Data which the College must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

7.5 The College recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. The College has a Rights of Individuals Policy and a Rights of Individuals Procedure which set out how the College responds to requests relating to these issues. Any request from an individual for the amendment, rectification, erasure or restriction of the use of their Personal Data should be dealt with in accordance with those documents.

7.6 Personal Data must not be kept for longer than it is needed

7.7 Data Protection Laws require that the College does not keep Personal Data longer than is necessary for the purpose or purposes for which the College collected it.

7.8 The College has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by the College, the reasons for those retention periods and how the College securely deletes Personal Data at the end of those periods. These are set out in the Data Retention Policy.

7.9 If College Staff feel that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, for example because there is a requirement of law, or if College Staff have any questions about this Policy or the College's Personal Data retention practices, they should contact the Data Protection Officer for guidance.

8.0 Record of Processing Activity (RoPA) and Information Asset Register

8.1 "Processing" is the collection, recording, organisation structuring, storage, adoption or alteration, retrieval, consultation or use, disclosure, destruction or erasure of personal data. The College will identify the legal basis for processing 'personal data' as defined by Article 6 and 'special categories of data' as defined by Article 9 and document this on a Record of Processing Activity (ROPA) through an Information Asset Register as required by Article 30.

8.2 The College will assess which lawful purpose applies to make each use of personal data lawful. If the use changes then the assessment will need to be updated. The use of personal data will be reviewed periodically, and any initial data audits will be updated periodically too.

8.3 If the College is considering making changes, we will decide whether their intended use requires amendments to be made and any other controls which need to apply, and we may need to notify Individuals (Data Subjects) about the change.

8.4 The College will undertake an Annual Data Audit, as required by the Act, to ensure that information is being collected, handled and stored in accordance with this Policy. Information from the audit will be used to update the RoPA. This audit will be undertaken internally.

9.0 Data Security

9.1 The College takes information security very seriously and the College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

9.2 The College has an Information Security Policy that staff must adhere to in order to ensure personal information held on the College's network is protected from unauthorised viewing and from loss.

9.3 The College has achieved the ISO27001 kitemark for information security and the maintenance and expansion of this kitemark is seen as a major part of the College's processes and systems to keep data secure.

9.4 Where electronic files need to be shared, the following should be ensured:

- Any sensitive personal information sent by email should be password protected as a minimum, with the password delivered to the recipient using a method other than email
- Whenever possible, the information should be shared via an exclusive link through Office 365

9.5 6.1 Paper records containing personal information should be minimised, but where these need to be kept the following should be carried out:

- Use of lockable cupboards (with restricted access to keys)
- Minimisation of personal data taken off site and ensuring it is transported and stored as

securely as possible
- Correct use of confidential waste services

10.0 Data Breach

10.1 Whilst the College takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens there will be a Personal Data breach and College Staff must comply with the College's Data Breach Notification Process (see Appendix B). Please see paragraph 9.6 for examples of what can be a Personal Data breach. Please familiarise yourself with it as it contains important obligations which College Staff need to comply with in the event of Personal Data breaches.

10.2 Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal to the organisation does.

10.3 The ICO states: "*A personal data breach may, if not addressed in an appropriate and timely manner, 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*."

10.4 A Personal Data breach can cause emotional distress as well as physical and material damage and can significantly affect individuals whose personal data has been compromised. However not all personal data breaches will lead to such outcomes. Each case needs to be assessed individually by looking at all relevant factors.

10.5 Once a breach is reported and an assessment carried out resulting in a risk to an individuals' rights and freedoms then the ICO must be notified. This must do this within 72 hours of becoming aware of the breach, where feasible, either by telephone or online outside of office hours.

10.6 There are three main types of Personal Data breach which are as follows:

- **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a College Staff is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;
- **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service

attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and

- **Integrity breach** - where there is an unauthorised or accidental alteration of Personal Data.

11.0 Appointing Contractors who Access the College's Personal Data

11.1 If the College appoints a contractor who is a Processor of the College's Personal Data, Data Protection Laws require that the College only appoints them where the College has carried out sufficient due diligence and only where the College has appropriate contracts in place.

11.2 One requirement of UK GDPR is that a Controller must only use Processors who meet the requirements of the UK GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

11.3 Any contract where an organisation appoints a Processor must be in writing.

11.4 You are considered as having appointed a Processor where you engage someone to perform a service for you and as part of that service they may get access to your Personal Data. Where you appoint a Processor you, as Controller remain responsible for what happens to the Personal Data.

11.5 UK GDPR requires the contract with a Processor to contain the following obligations as a minimum:

- to only act on the written instructions of the Controller;
- to not export Personal Data without the Controller's instruction;
- to ensure staff are subject to confidentiality obligations;
- to take appropriate security measures;
- to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;
- to keep the Personal Data secure and assist the Controller to do so;
- to assist with the notification of Data Breaches and Data Protection Impact Assessments;
- to assist with subject access/individuals rights;
- to delete/return all Personal Data as requested at the end of the contract;
- to submit to audits and provide information about the processing; and
- to tell the Controller if any instruction is in breach of the UK GDPR

11.6 In addition the contract should 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 individuals; and

- the obligations and rights of the Controller.

12.0 Individual's Rights

12.1 GDPR gives individuals more control about how their data is collected and stored and what is done with it. Some existing rights of individuals have been expanded upon and some new rights have been introduced. It is extremely important that Colleges plan how they will handle these requests under GDPR.

12.2 Subject Access Requests

- Individuals have the right under the GDPR to ask a College to confirm what Personal Data they hold in relation to them and provide them with the data. This is not a new right but additional information has to be provided and the timescale for providing it has been reduced from 40 days to one month (with a possible extension if it is a complex request). In addition, you will no longer be able to charge a fee for complying with the request.
- Subject Access Requests are becoming more and more common and are often made in the context of a dispute which means that it is crucial that they are handled appropriately to avoid a complaint being made to the ICO.
- Annex A outlines the procedure for handling a Subject Access Request.

12.3 The different types of rights of individuals are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (the right to be forgotten)
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Right to be informed

12.4 The information you supply about the processing of personal data must be:

- Concise, transparent, intelligible and easily accessible
- written in clear and plain language, particularly if addressed to a child
- Free of charge
- However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

Right of Rectification and Erasure (Right to be Forgotten)

This is a limited right for individuals to request the erasure of Personal Data concerning them where:

- the use of the Personal Data is no longer necessary under the purpose it was originally collected;
- their consent is withdrawn;
- the individual objects to the processing and there are no overriding legitimate grounds for the processing;
- the Personal Data has been unlawfully processed;
- the Personal Data has to be erased for compliance with a legal obligation.

12.5 The College can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes;
- the exercise or defence of legal claims.

12.6 All staff, students and other users are entitled to know:

- What information the College holds and processes about them and why it processes it;
- How the information can be accessed;
- How the information is kept it up;
- How the College is complying with its obligations under the GDPR 2018 Act.

12.7 The College must be prepared to answer the following kind of queries:

- "Do you hold data about me and can I have access to that data?"
- "Why do you hold data about me?"
- "Do you disclose my data to anyone else?"

12.8 Staff, students and other users of the College have the right to access any personal data that is being kept about them either on a computer or in any 'relevant filing system'. Any person who wishes to exercise this right should complete the College Data Subject Access Request form (See Annex C).

Right of Data Portability

12.9 An individual has the right to request that data concerning them is provided to them in a safe, structured, commonly used and IT compatible format.

12.10 If the individual requests it, the college may be required to 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.

12.11 This right is different to a subject access and is intended to give individuals a subset of their data.

Right to Object

12.12 The College will use all Personal Data in accordance with the rights given to Individuals under Data Protection Laws, and will ensure that it allows Individuals to exercise their rights in accordance with the College's Rights of Individuals Policy and Rights of Individuals Procedure. Please familiarise yourself with these documents as they contain important obligations which College Staff need to comply with in relation to Individuals' rights over their Personal Data.

13.0 Marketing and Consent

13.1 The College will sometimes contact Individuals to send them marketing or to promote the College. Where the College carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.

13.2 Marketing consists of any advertising or marketing communication that is directed to particular individuals. GDPR requires that organisations that market to individuals:

- Provide detail in their privacy notices, including for example whether profiling takes place;
- Have clear rules on obtaining consent require an individual's "clear affirmative action". The ICO like consent to be used in a marketing context.

13.3 Colleges also need to be aware of the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection. PECR apply to direct marketing i.e. a communication directed to particular individuals and covers any advertising/marketing material. It applies to electronic communication i.e. calls, emails, texts, faxes. PECR rules apply even if you are not processing any personal data.

13.4 Consent is central to electronic marketing. Best practice suggests that consent is gained by providing an un-ticked opt-in box.

14.0 Automated Decision Making and Profiling

14.1 Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.

- **Automated Decision Making** happens where the College makes a decision about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects; and
- **Profiling** happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

14.2 Any Automated Decision Making or Profiling which the College carries out can only be done once the College is confident that it is complying with Data Protection Laws. If College Staff therefore wish to carry out any Automated Decision Making or Profiling College Staff must inform the Data Protection Officer.

14.3 College Staff must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

14.4 The College does not carry out Automated Decision Making or Profiling in relation to its employees.

15.0 Data Protection Impact Assessments (DPIA)

15.1 The GDPR introduce a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment ("DPIA"). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

- Describe the collection and use of Personal Data;
- Assess its necessity and its proportionality in relation to the purposes;
- Assess the risks to the rights and freedoms of individuals; and
- The measures to address the risks.

15.2 A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. The ICO's standard DPIA template is available from www.ico.org.uk.

15.3 Where a DPIA reveals risks which are not appropriately mitigated the ICO must be consulted.

15.4 Where the College is launching or proposing to adopt a new process, product or service which involves Personal Data, the College needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The College needs to carry out a DPIA at an early stage in the process so that the College can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

15.5 Situations where the College may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):

- Large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;
- Large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data; or
- Systematic monitoring of public areas on a large scale e.g. CCTV cameras.

15.6 All DPIAs must be reviewed and approved by the Data Protection Officer.

16.0 Transferring Personal Data to a County Outside of the EEA

16.1 Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA. It needs to be thought about whenever the College appoints a supplier outside the EEA or the College appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA.

16.2 So that the College can ensure it is compliant with Data Protection Laws College Staff must not export Personal Data unless it has been approved by the Data Protection Officer.

16.3 College Staff must not export any Personal Data outside the EEA without the approval of the Data Protection Officer.

17.0 DEFINITIONS

College – South Staffordshire College

College Personnel – Any College employee, worker or contractor who accesses any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.

Controller – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data.

A Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data the College is the Controller of include employee details or information the College collects relating to students. The College will be viewed as a Controller of Personal Data if it decides what Personal Data the College is going to collect and how it will use it.

A common misconception is that individuals within organisations are the Controllers. This is not the case it is the organisation itself which is the Controller.

Data Protection Laws – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

EEA – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

ICO – the Information Commissioner's Office, the UK's data protection regulator.

Individuals – Living individuals who can be identified, directly or indirectly, from information that the College has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.

Personal Data – Any information about an Individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context.

Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as firstname.surname@organisation.com), IP address and also more sensitive types of data such as trade union membership, genetic data and religious beliefs. These more sensitive types of data are called "Special Categories of Personal Data" and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.

Processor – Any entity (e.g. company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller.

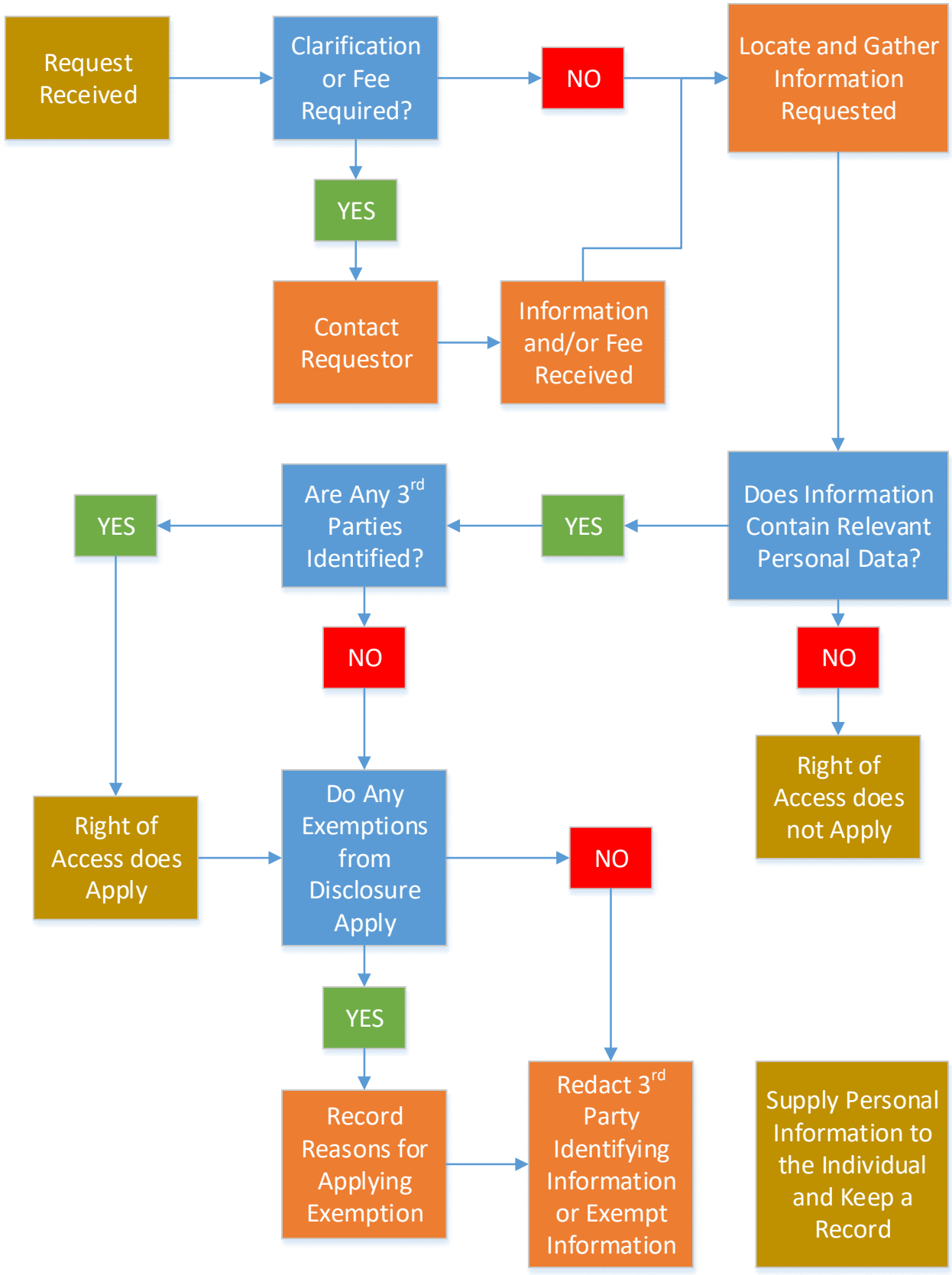
A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include: where software support for a system, which contains Personal Data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services.

Record of Processing Activities (RoPA) – The RoPA sets contains all the relevant requirements set out in Article 30 of the UK GDPR and should include as a minimum an organisation's name and contact details, whether it is a controller or a processor (and where applicable, the joint controller, their representative and the DPO). It should also:
outline the purposes of the processing

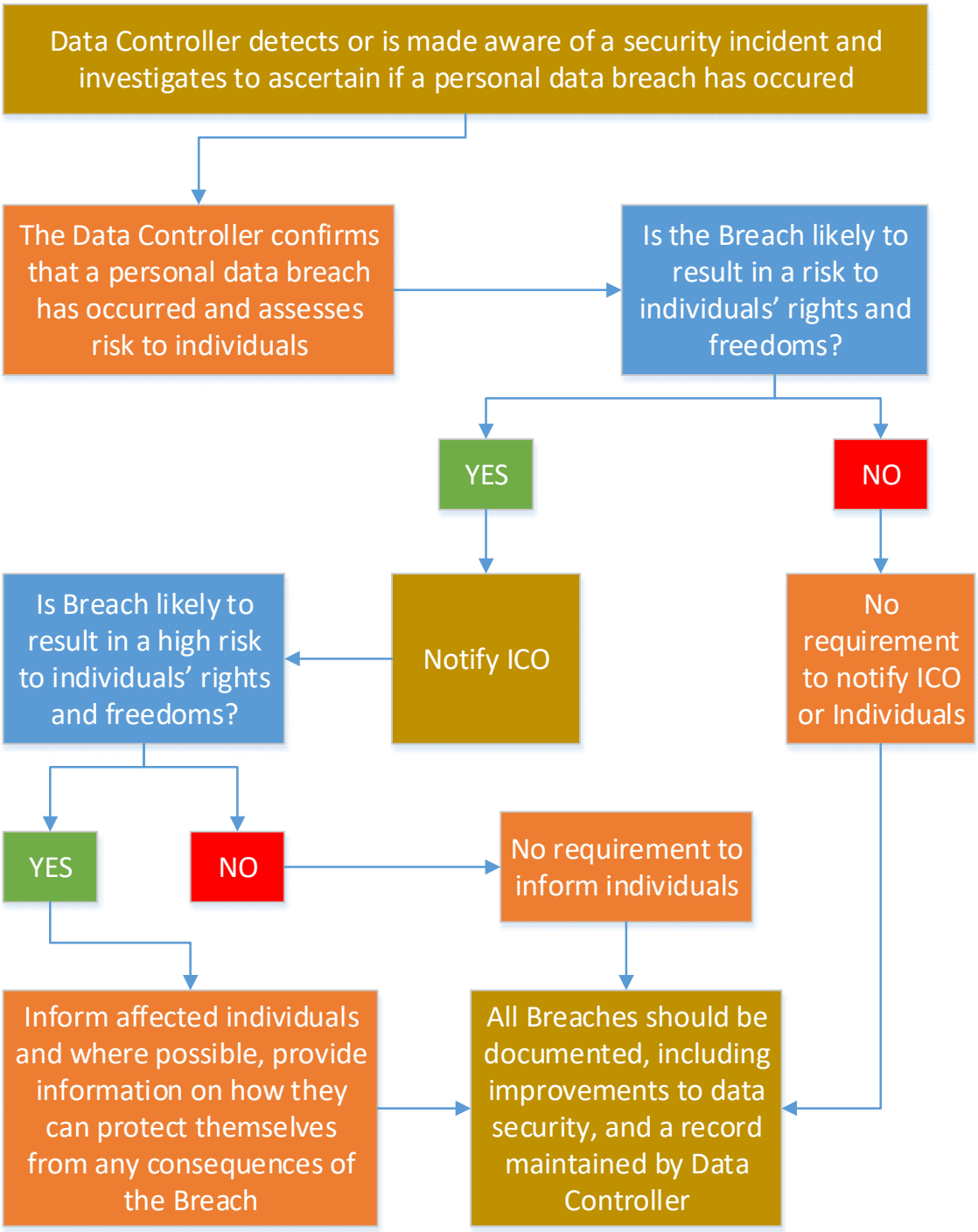
- A description of the categories of individuals and of personal data;
- The categories of recipients of personal data;
- Details of transfers to third countries, including transfer mechanism safeguards in place;
- Retention schedules; and
- A description of the technical and organisational security measures in place.

Special Categories of Personal Data – Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

APPENDIX 1 – SUBJECT ACCESS REQUEST FLOWCHART



APPENDIX 2 – DATA BREACH FLOWCHART



APPENDIX 3 – SUBJECT ACCESS REQUEST FORM

NAME	
PHONE	
EMAIL	
ADDRESS	
EMPLOYEE or STUDENT Number	

By completing this form, you are making a request to South Staffordshire College under the General Data Protection Regulations for eligible information which the College holds about you.

Please provide details on the information you require including (where possible) dates and any other evidence you have. We will be able to process your request more quickly if the information required is clear and well defined.

By signing below, you are confirming that you are the Individual named above. The College cannot accept Subject Access Requests from anyone other than the Individual including family members. You confirm that if you are not the individual named above, you will fully indemnify the College for any losses, costs and expenses occurring as a result of impersonating the Individual.

The College may need to contact you to confirm your identity before responding to your request.

Data Subject Signature	
Date	