STOKE ON TRENT COLLEGE	**POLICY 49** **DATA PROTECTION POLICY**	

1. Introduction

Stoke on Trent College (the College) is committed to protecting the rights and freedoms of data subjects (natural persons), the safe and secure processing of their data, in accordance with Data Protection Legislation. The College's reputation and future growth are dependent on the way the College manages and protects Personal Data. Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the College.

Data Protection Legislation means the Data Protection Act 2018 which incorporates the General Data Protection Regulation (GDPR) 2016, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the General Data Protection Regulation which is the governing legislation that regulates data protection across the EEA. This includes any replacement legislation coming into effect from time to time.

This policy sets out how we seek to protect personal data and ensure that our employees understand the rules governing their use of the Personal Data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

The College's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all of our employees to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action.

The College collects, uses and stores Personal Data about its students, prospective students, alumni, parents / guardians, employees, job applicants, visitors, sole traders, partnerships that supply the College, and individual representatives of companies that supply the College, Corporation Members and customers who use our hair, beauty or restaurant facilities, 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 GDPR.

As an organisation that collects, uses and stores Personal Data about its students, prospective students, alumni, parents / guardians, employees, job applicants, visitors, sole traders, partnerships that supply the College, and individual representatives of companies that supply the College, Corporation Members and customers who use our hair, beauty or restaurant facilities, 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 GDPR.

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 will provide for a successful working and learning environment for all.

College Staff 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 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.

If you have any queries concerning this Policy, please contact our Data Protection Officer, who is responsible for ensuring the College's compliance with this Policy.

This policy has been approved by the College's Principal and CEO, Lisa Capper, and the Chair of the Corporation Board, Jeremy Cartwright

2. Scope

This policy applies to all processing of personal data whether;

- wholly or partly by automated means (i.e.by computer) or
- by other means (i.e. paper records) that form part of filing system or are intended to form part of a filing system.

This policy applies to all staff, who must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to Internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

3. Definitions

- **Adequacy** – A term the EU uses to describe countries, territories, sectors or organisations it deems to have an "essentially equivalent" level of data protection to the EU. The EU Commission have adopted adequacy decisions for the UK GDPR and the Law Enforcement Directive. This means data can continue to flow freely from the EU to the UK, in the majority of cases.
- **College** – Stoke on Trent College

- **College Staff** – Any College employee, worker or contractor who accesses any of the College's Personal Data and will include employees, consultants, contractors, and temporary staff 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) is an EU regulation and no longer applies to the UK. The GDPR is retained in domestic law as the UK GDPR and sits alongside an amended version of the Data Protection Act 2018 Chapter 12[1] (DPA 2018). All applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice in the UK adhere to the amended version of the Data Protection Act 2-18 (DPA 2019)
- **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

[1] https://www.legislation.gov.uk/ukpga/2018/12/contents

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.

- **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

4. Who is responsible for this policy?

Our Data Protection officer (DPO) has overall responsibility for the day-to-day implementation of this policy. You should contact the DPO Lead in the first instance for further information about this policy if necessary.

- DPO Lead: **dpo@stokecoll.ac.uk**

5. Data protection principles

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;
- 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.
- 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.

6. Purpose

The purpose of this policy is to provide guidance on the data protection principles that all those acting on behalf of "The College" must adhere to when any personal data belonging to or provided by data subjects is collected, stored or transmitted.

It is therefore imperative that all those who access this policy, including employees and contractors and vendors, comply with the 6 Data Protection Principles (GDPR Article 5), summarised below.

I. Ensure that personal data is processed lawfully, fairly and in a transparent manner in relation to individuals. We will inform people what data we collect and why, through a Privacy Notice

II. Ensure that personal information is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. We will only process personal information for specific reasons, these include fulfilment of a contract (with a parent to provide childcare services or with an employee under their contract of employment)

III. Ensure that all information is adequate, relevant and limited to what is necessary in relation to the purposes for which it is collected

IV. Ensure that all information is kept accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay

V. Ensure that kept data is kept for no longer than is necessary for the purposes for which it is being processed. Ensure information is protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and operational measures

VI. Demonstrate compliance with these requirements through appropriate documentation, training, spot checks and audits

7. Our Procedure

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

8. Lawful basis for processing data

We must establish a lawful basis for processing data.

Employees must ensure that any data they are responsible for managing or working with has a written lawful basis approved by the DPO.

At least one of the following conditions must apply whenever we process personal data:

1. **Consent**
   We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
2. **Contract**
   Processing is necessary to fulfil or prepare a contract for the individual.
3. **Legal obligation**
   Processing is necessary to meet a legal obligation (excluding a contract).
4. **Vital interests**
   Processing is necessary to protect a person's life or in a medical situation.
5. **Public function**
   Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. **Legitimate interest**
   Processing is necessary for the College's legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

9. Deciding which Condition to Rely on

If you are making an assessment of the lawful basis, you must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. You cannot rely on a lawful basis if you can reasonably achieve the same purpose by some other means.

Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.

Consider the following factors and document your answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

If you are responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, you must have this approved by the DPO.

10. Accountability

The College must ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle. You are responsible for keeping a written record of how all the data processing activities you are responsible for comply with each of the Principles. This must be kept up to date and must be approved by the DPO.

To comply with data protection laws and the accountability and transparency Principle of GDPR, we must demonstrate compliance. You are responsible for understanding your particular responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments
- Implement measures to ensure privacy by design and default, including:
- Data minimisation
- Pseudonymisation
- Transparency
- Allowing individuals to monitor processing
- Creating and improving security and enhanced privacy procedures on an ongoing basis

11. Controlling vs. Processing data

GDPR, the EU regulation that has been incorporated into UK domestic law, applies to data 'Controllers' and 'Processors'.

- A Controller determines the purposes and means of processing personal data.
- A Processor is responsible for processing personal data on behalf of a Controller.

"The College" is both a Controller and a Processor of data and as the Processor we have specific legal obligations placed upon us; e.g. we are required to maintain records of personal data and processing activities such as employee personnel records and as such we have a legal liability to protect this information and will be held responsible for a breach.

As a Controller, we are not relieved of our obligations where the Processor is involved (i.e. in a sub contract arrangement the College is the Controller, the Sub Contractor is the Processor) as GDPR places further obligations on us to ensure our contracts with Processors comply with GDPR.

GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for National Security purposes and processing carried out by individuals purely for personal/household activities.

12. Appointing Contractors who access the College's personal data

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.

One requirement of GDPR is that a Controller must only use Processors who meet the requirements of the 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

- Any contract where an organisation appoints a Processor must be in writing.
- 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 assist with the notification of Data Breaches and Data Protection Impact Assessments
- to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law

13. Special Categories of Data

What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

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

In most cases where we process special categories of personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

14. Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines. A copy of our Retention schedule can be obtained on request from the DPO.

15. Privacy Notices

When to supply a privacy notice

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which mean within one month.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

What to include in a privacy notice

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children The following information must be included in a privacy notice to all data subjects:

- Identification and contact information of the data controller and the data protection officer
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- Detailed information of any transfers to third countries and safeguards in place

- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and internal complaint procedures
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
- Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

16. Status of the Policy

This Policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College from time to time. Any failures to follow the Policy can therefore result in disciplinary proceedings.

Any member of staff who considers that the Policy has not been followed in respect of personal data about them, should raise the matter with the Data Protection Officer initially. If the matter is not resolved, it should be raised as a formal grievance.

Compliance with data protection law is the responsibility of all members of the College. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

17. Roles and Responsibilities

Senior Leadership Team

Overall accountability for data protection sits with the Executive Board

The Executive Board will:

a. Establish a data protection culture in the organisation

b. Ensure the College has appointed an appropriate Data Protection Officer

c. Ensure the Data Protection Officer operates independently and is not dismissed or penalised for performing their task (in relation only to their role as Data Protection Officer as defined in law)

d. Ensure that adequate resources are devoted to meet the College's data protection obligations

e. Commission reports from the Data Protection Officer and take action to remedy deficiencies identified by the report in a timely manner

Board of Governors

The Governors are responsible for holding the Senior Leadership Team to account to ensure compliance with the law.

The Data Protection Officer has a direct reporting line to the Governors where they can raise any data protection risks or compliance issues.

Data Protection Officer

Operational responsibility for data protection sits with the College's Data Protection Officer.

The Data Protection Officer will:

a. Inform and advise all members of staff on their data protection obligations

b. Monitor compliance with data protection requirements

c. Contribute to the development and maintenance of all data protection policies, procedures and processes in relation to the protection of personal data

d. Advise and inform the College on any data protection impact assessment (DPIA), including monitoring performance of DPIAs

e. Report and advise the Executive Board on the allocation of their responsibilities to support ongoing compliance Data Protection law

f. Provide data protection training and awareness to all members of staff

g. Conduct audits of processes relating to personal data

h. Be the point of contact for data subjects with regard to the processing of their personal data and respond to all data subject access request

i. Advise senior management on the allocation of information security responsibilities

j. Develop/advise on formal procedures for reporting incidents and investigations

k. Contribute to the risk management, business continuity and disaster recovery planning process

l. Advise on and monitor organisational record management and retention arrangements

m. Ensure that records of the processing are kept and the College Notifies the ICO

n. Advise on the issuing of privacy notices to data subjects at the point of collection of their personal data

o. Be the first point of contact for any enquiries from the Information Commissioners Office (and any other EU supervisory authorities)

Responsibilities of Staff

All staff will:

a. Ensure any personal data which they hold is kept securely

b. Ensure personal information is not disclosed either orally or in writing, accidentally or otherwise unlawfully to any unauthorised party

c. Only access personal data that is applicable and required for them to undertake their role

d. Complete and submit a data breach form at the first opportunity if and when any data breach
occurs

e. Undertake all required data protection training

f. Maintain data protection awareness at all times reporting any data protection risks or concerns to their Line Manager or the Data Protection Officer

g. Ensure that records are accurate, kept up to date kept securely and disposed of safely in accordance with the timescales set out in this policy

h. Only send marketing information if they have consent from the data subjects and approval from the Marketing Department and Data Protection Officer

i. Not process Special Categories of data or Criminal offence data without first ensuring they have a legal basis to do so and recording this processing with the Data Protection Officer j. Ensure they have an appropriate contract in place (approved by the Data Protection

Officer) with any third-party organisation that will have access to personal data

j. Check that any information that they provide to the College in connection with their employment is accurate and up to date and inform the College of any changes to information which they have provided, e.g. change of address or name l. Comply with the security measures set out as follows:

Security Measures:

Physical Security:

a. Staff must wear their ID badge at all times

b. Staff must never allow others to use their keys, swipe cards or pin numbers to gain entry

c. Staff must not allow others to 'tailgate' e.g. follow a staff member through secure areas

d. Staff must report to security personnel if they encounter unescorted visitors or anyone not wearing appropriate visible identification, (i.e. an ID badge).

e. Boards displaying person identifiable data should be sited in areas not accessible to the learners or the public

Paper Record Security:

a. All paper and files containing data subject details to be securely locked away when not in use and follow a "clear desk policy"

b. Data that is no longer required must be disposed of securely. The College uses a secure shredding company to dispose of data securely

Working remotely/offsite:

a. Copies of physical records must only be taken off-site where absolutely necessary

b. Only take the minimum necessary personal information off site

c. Never take the master records off-site (only copies of the parts of the record necessary for the purpose)

d. Ensure that staff members have a secure place to protect manual information

e. Never leave personal information in an unsecure area in the home, i.e. in garages, sheds, boots of cars, near open doors or windows

f. Never work on personal information in a public place where it could be seen by a third party

g. Prevent access to information by other members of the household and by visitors. Staff members working at home should ensure they adopt a clear desk policy when leaving their work unattended

Transporting Paper Records:

a. Keep information in a sealed container/bag

b. Public transport should not be used for transporting personal information, if an exception to this rule is identified the information must be transported in a locked briefcase or similar

c. Never leave information unattended in the car for an extended length of time

d. Never leave information in the boot of a car overnight. Information must be taken inside a property and secured

When sending information by post:

a. All external post should be delivered to the Post Room

b. Post should not be left in unsupervised areas that are open to learners or the general public

c. Post containing personal or confidential information should be sent in sealed envelopes and marked as CONFIDENTIAL

IT Security:

a. Screens of computers must always be locked when left unattended

b. If electronic data is stored on removable media (like a CD, DVD or USB pen drive), these must be encrypted and kept locked away securely when not in use

c. Electronic data should only be stored on the College's designated drives and servers and should only be uploaded to an approved cloud computing service (eg Microsoft 365 – incorporating OneDrive and Sharepoint which are subject to 2-factor authentication).

d. Logon credentials are individual and must not be used to provide system access to a third party (staff, student or visitor)

Sending information by email:

a. Consider if email is the best communication method.

b. Consider whether the e-mail going to just one person. If so, is it the correct person where similar names exist in the e-mail directory or address book

c. Consider whether to use the 'reply all' function. If so, does every person on the list need to receive the reply and any attachment.

d. Carefully check the recipients of all e-mails prior to sending regardless of content. Staff members should be extra vigilant where personal, sensitive personal or confidential information is included

e. Delete emails which they have reached their retention period

f. Only send email from another member of staff's email account or under an assumed name if they have the specific authority. This is generally reserved for personal assistants to Directors

g. Manage email appropriately; clearing the deleted items folder and using appropriate archiving facilities

h. Password protect the content of any email when sending sensitive/confidential/special categories of data

18 Learner Obligations

Learners must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes of address, etc., are notified to the personal tutor.

19 Rights of Data Subjects

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

Data Protection law provides a set of rights for data subjects. These are:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

These rights must be complied with within one month (this can be extended by two months where the request is complex). Where the timescale is extended the College must inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Detailed guidance on compliance with these rights is set out at Appendix 3 – Data Subjects Rights.

20 Subject Access Requests

What is a subject access request?

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information, which means the information, which should be provided in a privacy notice.

How we deal with subject access requests

- We must provide an individual with a copy of the information the request, free of charge. This must occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.
- If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. You must obtain approval from the DPO before extending the deadline.
- We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the DPO.
- Once a subject access request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

21 Data portability requests

We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and you must receive express permission from the DPO first.

22 Right to Erasure

What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

How we deal with the right to erasure

We can only refuse to comply with a right to erasure in the following circumstances:

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

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

23 The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.

- The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

24 Data audits

Regular data audits to manage and mitigate risks will be carried out. This includes information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. You must conduct a regular data audit as defined by the DPO and normal procedures.

25 Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. The College will keep this policy under review and amend or change it as required. You must notify the DPO of any breaches of this policy. You must comply with this policy fully and at all times.

26 Training

You will receive adequate training on provisions of data protection law specific for your role. You must complete all training as requested. If you move role or responsibilities, you are responsible for requesting new data protection training relevant to your new role or responsibilities. If you require additional training on data protection matters, contact the DPO.

27 Breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. The College has a legal obligation to report any data breaches to the Information Commissioner's Office within 72 hours.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures

- Notify the Information Commissioners Office of any compliance failures that are material either in their own right or as part of a pattern of failures

28 Compliance

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures, which may result in dismissal. Questions about the interpretation or operation of this policy should be taken up in the first instance with the Data Protection Officer.

Any individual who considers that the Policy has not been followed in respect of Personal Data about themselves should also raise the matter with the Data Protection Officer.

Further information about the DPA and the GDPR can be found on the Information Commissioner's Office (ICO website). **https://ico.org.uk/**

29 Data Protection Impact Assessments (DPIA)

Data protection impact assessments (also known as privacy impact assessments or DPIAs) are a tool which can help identify the most effective way to comply with data protection obligations. An effective DPIA will allow the College to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

The DPIA should be started as early as is practicable in the design of the processing operation even if some of the processing operations are still unknown. Updating the DPIA throughout the lifecycle project will ensure that data protection and privacy are considered and will encourage the creation of solutions which promote compliance.

The Data Protection Officer supports employees undertaking a DPIA and will provide advice and will monitor the performance of the DPIA.

Where appropriate the College shall seek the views of data subjects or their representatives e.g. affected customers, members, partner organisations or employees as part of undertaking the DPIA. Where appropriate the College will also consult with the ICO.

30 International Transfers

Data Protection law imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individual's data is not undermined. Where staff

are required to sending personal data to outside the European Union, to third countries or international organisations they must seek advice from the Data Protection Officer.

31 Breach Management

It is essential that all data protection incidents or near misses are handled appropriately. Where a data protection incident or potential incident has been identified staff should complete the form in Appendix 11 and forward this to the Data Protection Officer via dpo@stokecoll.ac.uk who will follow the process set out In the College Data Breach Policy.

32 References

ARTICLE 29 DATA PROTECTION WORKING PARTY: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679: 4 October 2017

http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

Information Commissioner's Office, Guide to the General Data Protection Regulation (GDPR), licensed under the Open Government Licence

33 Approval

Approved by the College Executive Team

Signed:

(Principal)

Endorsed by the College Corporation

Signed:

(Chair)

Appendix 1 – Key Definitions

Personal data	'personal data' means any information relating to an identifiable person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Special categories of personal data	'Special categories of personal data' are racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation. Note: This was previously referred to as Sensitive Personal data
Processing	'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Data Controller	'controller' any person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

Data Processor	'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
Data Protection law	Refers to the applicable laws of the land including once enforce the UK Data Protection Act 2018 and the EU General Data Protection Regulations

Appendix 2 –Criminal Offence Data

Data Protection law requires that the processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorised by law providing for appropriate safeguards for the rights and freedoms of data subjects.

The College must not process Criminal offence data unless it meets specific terms and conditions. Staff must not process Criminal offence data without first ensuring they have a legal basis to do so and recording this processing with the Data Protection Officer.

Appendix 3 – Consent & Marketing

In some cases, the College may need to rely on an individual's explicit consent to process their personal data.

Where the College is relying on Consent to process personal data it will ensure that:

a. Consent is the most appropriate lawful basis for processing
b. The request for consent is prominent and separate from other terms and conditions
c. We ask people to positively opt in
d. We don't use pre-ticked boxes or any other type of default consent
e. We use clear, plain language that is easy to understand
f. We specify why we want the data and what we're going to do with it

g. We give individual ('granular') options to consent separately to different purposes and types of processing

h. We name our organisation and any third-party controllers who will be relying on the consent

i. We tell individuals they can withdraw their consent

j. We ensure that individuals can refuse to consent without detriment

k. We avoid making consent a precondition of a service

Marketing

There are specific rules around sending advertising or marketing material which is directed to specific individuals.[3] Routine service messages do not count as direct marketing – in other words, correspondence to provide information they need about the College (e.g. information about college closures due to bad weather, safety announcements, changes to term dates etc.). General branding, logos or straplines in these messages do not count as marketing.

When sending specific marketing message, the College must obtain consent to send any emails, texts, picture messages, video messages, voicemails, direct messages via social media or any similar electronic messages.

Consent must be obtained in line with the process set out in this Policy. All marketing projects must be approved by the Data Protection Officer and Marketing Department.

Privacy and Electronic Communication (Amendment) Regulations 2018[2]
The Privacy and Electronic Communications (EC Directive) Regulations 2003[3]

Appendix 4 – Privacy

In some cases, it will be appropriate to include a specific statement on data collection forms used by the College. A template statement is provided below. Staff must ensure that they provide the Data Protection Officer a copy of any template data collection forms which include the Privacy Statement so that a central register can be maintained.

[2] https://www.legislation.gov.uk/uksi/2018/1189/contents/made
[3] https://www.legislation.gov.uk/uksi/2003/2426

Template Privacy Statement

Stoke on Trent College collects your [what personal details e.g. name, address, date of birth] so that we can [high level reason for collecting the details].

We collect and use your information [specific reasons for collecting the details].

We will share this personal data with [people/companies we share the data with] for the purpose of [reason]. Your data [will not be sent outside of the UK.] / or [will be transfer to (name of countries)].

We will retain this information in line with the retention timescales set out in our Data Protection Policy.

You have a number of rights under data protection law including the right to be informed, right of access, right to rectification, right to erase, right to restrict processing, right to data portability, right to object and rights in relation to automated decision making and profiling.

If you have any questions about the use of your personal data please see our Privacy Notice or contact our Data Protection Officer (dpo@stokecoll.ac.uk). If you are unhappy with our handling with your personal data, you have the right to make a complaint to the Information Commissioners Office.

Appendix 5 – Publication

Publication of College Information

It is the policy of the College to disclose relevant information to the public; in particular, the following information will be available to the public for inspection:

a. names and photographs of College governors;

b. names and contact details of the Executive Board member / Principalship

c. the information published in accordance with the College's publication scheme adopted pursuant to the Freedom of Information Act 2000

Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Data Protection Officer.

Appendix 6 – Principles

Principle 1

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

If you are responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, you must have this approved by the DPO.

Principle 2 – Specific and explicit purposes

This principle aims to ensure that organisations are open about their reasons for obtaining personal data, and that what they do with the information is in line with the reasonable expectations of the individuals concerned.

In practice, the second data protection principle means that the College must:

a. be clear from the outset about why we are collecting personal data and what we intend to do with it

b. comply with the fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data

c. notifying the Information Commissioner of our processing

d. ensure that if we wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair

Principle 3 – Adequate, relevant and necessary

The College must ensure that all personal data collected is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Staff must ensure that they are only collecting the minimum data for the purpose for which it is required.

Principle 4 – Accurate and up to date

The College is required to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all staff who collect and use personal data to take reasonable steps to ensure it is kept up to date as possible.

All data should be held centrally; unnecessary duplicate or additional sets of data should not be created or filed separately. The College will prompt learners and staff to update their details.

A template form has been provided in Appendix 6 for learners to submit a change of details.

Principle 5 – Retention

The College will ensure that personal data is kept no longer than is necessary.

Records which have reached the end of their life (whether held in electronic or paper format) should generally be destroyed under confidential conditions. Once a document reaches its retention period it should be reviewed to ensure it does not need to be kept for longer as some records need to be kept for historical purposes and these will be transferred to a place of deposit by the Data Protection Officer. Any staff wishing to retain a record for longer than the specified retention period should contact the Data Protection Officer for advice and guidance.

A Document Retention Policy has been produced and staff must review this policy and ensure records are kept in line with the timescales specified. Staff must ensure that once data has reached its retention period it is destroyed securely. All personal data held in paper form must be disposed of by shredding or in the shred bins provided on College premises.

Electronic media will be disposed of securely by the IT department.

Principle 6 – Security

The College will ensure that data is 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.

Appendix 7 – Compliance with Data Subject Rights The right to be informed

The right of access

Data subjects have the right to access personal data that is currently being kept about them. Any person who wishes to exercise this right should complete the College 'Access to Data' form (See Appendix 5) and submit it to the Data Protection Officer.

The Data Protection Officer will log the request on the College's SAR database and liaise with the required departments to collate the personal data.

There are some limited exemptions which allow the College to withhold certain data (these can only be applied by the Data Protection Officer); however, generally all information should be supplied.

Disclosing personal data (Section 29 Forms)

The College is permitted to disclose personal data for the purposes of Crime and taxation. In the event that a section 29 form is received this must be immediately forwarded to the Data Protection Officer for action.

The right to rectification

The right to rectification gives data subjects the right to have personal data rectified if it is inaccurate or incomplete. If a data subject requests the College rectify inaccurate or incomplete data, the request must be sent to the Data Protection Officer for review. The Data Protection Officer will liaise with the relevant department to have the data rectified.

If the College has disclosed the inaccurate or incomplete personal data to any third parties, the College shall inform them of the rectification where possible. The Data Protection Officer shall inform the data subjects about the third parties to whom the data has been disclosed (where appropriate).

The right to erasure

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable a data subject to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The right to erasure does not provide an absolute 'right to be forgotten'.

Data subjects have a right to have personal data erased and to prevent processing in specific circumstances:

a. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed

b. When the data subject withdraws consent

c. When the data subject objects to the processing and there is no overriding legitimate interest for continuing the processing

d. The personal data was unlawfully processed

e. The personal data has to be erased in order to comply with a legal obligation

f. The personal data is processed in relation to the offer of information society services to a child

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

a. to exercise the right of freedom of expression and information

b. to comply with a legal obligation for the performance of a public interest task or exercise of official authority

c. for public health purposes in the public interest

d. archiving purposes in the public interest, scientific research historical research or statistical
purposes

e. the exercise or defence of legal claims

If the College has disclosed the personal data in question to third parties, the College will inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

The right to restrict processing

Data subjects have a right to 'block' or suppress processing of personal data. When processing is restricted, the College is permitted to store the personal data, but not further

process it. The College will retain enough information about the data subject to ensure that the restriction is respected in future but no further information.

The College is required to restrict the processing of personal data in the following circumstances:

a. Where a data subject contests the accuracy of the personal data, the organisation restricts the processing until it has verified the accuracy of the personal data

b. Where a data subject has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the organisation is considering whether our legitimate grounds override those of the data subject

c. When the processing is identified to be unlawful and the data subject opposes erasure and requests restriction instead

d. Where the organisation no longer needs the personal data, but the data subject requires the data to establish, exercise or defend a legal claim

If the College has disclosed the personal data in question to third parties, the College shall inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The College shall inform data subjects when it lifts a restriction on processing.

The right to data portability

The right to data portability allows data subjects 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.

The right to data portability only applies:

a. to personal data an individual has provided directly to the organisation

b. where the processing is based on the individual's consent or for the performance of a contract and

c. when processing is carried out by automated means (on a computer)

d. Where a data subject requests a copy of their personal data in a portable form the College will supply the data held in a structured, commonly used and machine-readable form.

Generally, this will be a CSV file from the College's computer systems. The information will be provided free of charge.

e. If the data subject requests it and if it is technically feasible, the College shall securely transmit the data directly to another organisation.

f. If the personal data concerns more than one individual, the Data Protection Officer will consider whether providing the information would prejudice the rights of any other individual.

The right to object

Data Subjects have the right to object to:

a. processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling) c. direct marketing (including profiling)

d. processing for purposes of scientific/historical research and statistics

In the event that an objection to processing is received this should be immediately forwarded to the Data Protection Officer who will consider and where required coordinate the ceasing of processing.

Where a request is received the College will stop processing the personal data unless:

a. we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or

b. the processing is for the establishment, exercise or defence of legal claims.

Rights in relation to automated decision making and profiling

Data Protection law includes specific rules where the College is conducting automated individual decision-making (making a decision solely by automated means without any human involvement); and/ or profiling (automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements).

Wherever the College wishes to use automated decision making and/or profiling the College will carry out a DPIA to identify the risks to individuals, show how we are going to deal with them and what measures we have in place to comply with the law.

Appendix – 8 Parents / Guardians / Carers

Learners are advised that it is college policy that staff may contact named parents/guardians of learners under the age of 18 at the start of the course to discuss academic progress, attendance and conduct. Learners who do not wish the college to make such contact may be granted an exemption by writing to the Principal at the commencement of their course.

The faculty administrators will provide a list of such learners which will be circulated to faculty managers and appropriate team leaders. If the learner has requested that the college does NOT contact their parents/guardians, then no information can be given.

The learner will have indicated on the enrolment form the name of the parent/guardian with whom contact can be made. Learners can change these details by submitting the form at Appendix 6.

Enquiries can be dealt with, generally by the Personal Tutor, but only with the person given by the learner using the contact details on the learner record.

Key Point: Staff should generally not give any information about a learner, not even confirmation that an individual is a learner at the college, in response to any telephone enquiry, even if the query is from the parents unless they have taken steps to verify the caller such as asking for specific information, such as learner date of birth, course attending etc.

Wherever possible it is recommended that staff:

a. Take the name and telephone number of the person calling

b. Ask the nature of the enquiry

c. Tell the caller that you will pass on the enquiry or telephone them back

Enquiries about a learner's progress or attendance should be passed on to the Personal Tutor

d. After the initial telephone enquiry, the lecturer or other staff member should check whether or not the learner wishes the college to contact parents

e. If the learner has opted out of parental contact, then the Personal Tutor should inform the learner that an enquiry has been made and urge the learner to discuss the matter with the parent

f. If the learner has not opted out of parental contact, then the Personal Tutor or other appropriate staff member should contact the parent (i.e. the person given by the learner on the enrolment form), using the telephone number that is on the learner record g. Other Family Members, Friends etc

Staff should not respond to any enquiries from other family members or friends and should not even confirm that someone is a learner at the college. If the reason for the enquiry is stated to be an emergency, then the matter should be referred to a member of the Executive Board.

Potential Employers and Education Institutions - Reference Requests

These should be dealt with by the Personal Tutor. All reference requests and responses should be in writing. The learner is entitled to see copies of any reference written about them.

See separate guidelines on the writing of references. Copies of all references should be kept in the learner file.

Government Agencies

Government agencies can include, but not be limited to, Social Services, Police, Benefits agencies, probation service, tax etc.

The College is legally bound to provide information to various government agencies. All requests for information and all responses should be in writing. Copies of all requests should be kept, preferably in the learner file.

Staff should seek advice from the Data Protection Officer when responding to any such requests.

Appendix 9 – Access to Data Request Form

You have the right under Data Protection law to see personal information that we hold about you. Please complete the details below to enable us to identify you and your information.

Full name (s) (include any previous known names)	
Current address	
Previously known address(s)	
Contact tel. and/or email	
Date of birth(s)	
Course undertaken	
Learner no(s)	
Dates attended	
To help us locate your information quickly please provide as much detail as possible about the type of information required	
Where the information is held in an electronic form would you like the data provided to you electronically	Yes / No
Data Subject(s) Declaration:	Signed…… Date……

Please provide two items of current identification confirming your signature and current address (e.g. passport or driving licence, and utility bill) in order for your request to be processed. If the information is insufficient or incomplete to action your request the statutory time frame will be suspended, whilst further information is collated from you.

The College has a statutory one month (this can be extended by two months where the request is complex) to comply with a Data Subject Access Request, this time frame will only commence when the College is in receipt of this form and the required identification documents. Where the timescale is extended the College will inform you of any such extension.

Data Subject's Representative

If you are seeking information about someone who is unable to contact the College directly please provide the Data Subject's written consent and current identification confirming their signature and current address, or appropriate Court Order or Power of Attorney.

Please complete the details below if you are acting as the representative to the data subject.

Full name/Organisation	
Address	
Relationship to data subject	
Contact tel. no. or email	
Data Subject Representative Declaration: I confirm that I am acting as the data subject's representative and include the appropriate consent document(s) and identification for them. Signed …… Date……	

Please forward all completed request forms and copies of ID to: Email:
dpo@stokecoll.ac.uk
Or via post to:
Data Protection Officer Stoke on Trent College
Cauldon Campus
Stoke Road
Shelton
Stoke on Trent
ST4 2DG

Appendix 10 – Learner Details Amendment Form

Additional or Replacement Contact

On the enrolment form, you provided your personal details; however, if these have changed please complete this form and give it to your Personal Tutor.

Details	Current	Revised
Your name		
Address		
Postcode		
College Course		N/A
Name of Personal Tutor		N/A
Name of Parent/Guardian/Carer		
Parent/Guardian/Carer Address		
Parent/Guardian/Carer Telephone		
Is this a **replacement** to the original name or an **addition**?		
Your signature		
Date		

Appendix 11 – Data Breach Notification Form

Notification of the breach

Data Protection law places a duty on the College to report certain types of personal data breach to the ICO within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the organisation must also inform those individuals without undue delay.

Data Breach/Near Miss Submission Form

Please complete as much information as possible and send the form to dpo@stokecoll.ac.uk

Incident / breach details	
Name of person reporting incident:	
Contact details of person reporting incident:	
Date(s) incident took place:	
Date you detected the incident:	
Place of incident:	

Brief description of how you became aware of the incident:	
Brief description of the incident including details of the data, records or systems believed to be affected:	
Approximate number of affected data subjects, if known:	
Approximate number of affected records, if known:	
Any actions taken in response to the incident:	

Thank you for reporting this incident. The Data Protection Officer will respond as soon as possible with advice and next steps on managing this incident.