UTC South Durham Data Protection Policy

Date of adoption	June 2018
Approved by	Governing Body
Signed: (Principal) 	**Date:** 1st June 2018
Signed: (Chair of Governors) 	**Date:** 1st June 2018

Date to be reviewed by	June 2020
Reason for Review	Bi- Annual
Responsibility	Business Manager

1. Introduction

The UTC South Durham acts as a Data controller for information collected to educate students. UTC South Durham is legally required to collect and process specific information about its employees, students and other users to allow it to discharge it's legal duties. These duties include; providing an education for students, reporting assessment and achievement to parents, safeguarding students, providing careers guidance and ensuring Health and Safety legislation is complied with. It is also necessary to process information so that staff can be recruited and paid, courses organised and to ensure legal obligations to funding bodies and government are complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the UTC must comply with the data protection principles which are set out in the General Data Protection Regulations (GDPR), May 2018. In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- Be adequate, relevant and not excessive for those purposes
- Be accurate and kept up to date
- Not to be kept longer than is necessary for that purpose
- Be processed in accordance with the data subject's rights
- Be kept safe from unauthorised access, accidental loss or destruction
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The UTC and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, The UTC has developed its Data Protection Policy.

2. Guiding principles

The aims of the policy include the following:

- To explain how data is held and processed
- To explain the responsibilities of staff under GDPR
- To explain the principles of data security
- To explain student obligations
- To provide information relevant to the rights of access to information
- To state how and what information will be published
- To explain the process of data collection to ensure subject consent is obtained
- To provide information on the processing of sensitive information
- To provide details on the college's data controllers for both staff and student issues
- To state the position in respect of student assessment results
- To provide information on the retention of data.

3. 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 UTC from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings, including dismissal.

Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated data controller initially. If the matter is not resolved it should be raised as a formal grievance.

4. Notification of data held and processed

All staff, students and other users are entitled to:

- Know what information the UTC holds and processes about them and why
- Know how to gain access to it and amend if required
- Know how to keep it up to date
- Know what the UTC is doing to comply with its obligations under the GDPR.
- Know how to with withdraw consent if required
- Know how to make a 'Subject Access Request'

The UTC will therefore provide all new staff with a standard form of notification. This will state all the types of data the UTC holds and processes about them, and the reasons for which it is processed.

5. Responsibilities of staff

All staff are responsible for:

- Checking that any information that they provide to the UTC in connection with their employment is accurate and up to date
- Informing, and providing supporting evidence to the UTC of any changes to information, which they have provided. e.g. changes of name/address
- Checking the information that the UTC will send out from time to time, giving details of information kept and processed about them
- Informing the UTC of any errors or changes. The UTC cannot be held responsible for any errors unless the staff member has informed the UTC of them.

If and when, as part of their responsibilities, staff collect information about other people, (i.e. about students course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff, which are set out in appendix 1.

6. Data security

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. Disclosures should be notified to the Information Commissioners office within 72hrs, via the DPO.

Personal information should be:

- Kept in a locked filing cabinet or
- In a locked drawer or
- If it is computerised, be password protected or
- Kept only on disk which is encrypted and is itself kept securely

7. Student and Parent obligations

Students and Parents must ensure that all personal data provided to the UTC is accurate and up to date. They must ensure that changes of address, etc. are notified to the and office manager.in the main office

Students who use the UTC computer facilities may, from time to time, process personal data. If they do they must notify the data controller. Any student who requires further clarification about this should contact the Business Manager.

8. Rights to access information

Staff, students and other users of the UTC have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should contact the make a subject access request. This subject access request should be made in writing to Jean Bell at UTC South Durham.

The UTC must comply with requests for access to personal information as 30 school working days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

9. Publication of UTC South Durham Data

Information that is already in the public domain is exempt from GDPR. It is the UTC's policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

- Name and contacts of UTC Governors
- List of staff
- Photographs of key staff.

The UTC internal phone list will not be a public document.

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

10. Subject consent

In most cases, the UTC can process personal data without the consent of the individual as it is our public task to provide an education and to discharge our legal obligations to staff.. Regardless of the basis for consent, data subjects still have all the data protection rights outlined in the relevant privacy statement.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 14 and 18. The UTC has a legal duty to ensure that staff are suitable for the job, and students for the courses offered. The UTC also has a duty of care to all staff and students and must therefore make sure that

employees and those who use the UTC facilities do not pose a threat or danger to other users. UTC South Durham will require an enhanced DBS for all staff to ensure that it meets its safeguarding obligations. Please see the Data Retention Policy regarding the erasure and destruction of information provided to carry out these checks.

The UTC may also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The UTC will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

Therefore, all prospective staff and students will be asked to sign a 'Consent to Process' Form, regarding particular types of information when an offer of employment or a course place is made available. A refusal to sign such a form can result in the offer being withdrawn.

11. Processing sensitive data (Special Category Data)

Sometimes it is necessary to process information about a person's health/disability, criminal convictions, race, gender, religion, sexual orientation, transgender and family details.

This may be to ensure the UTC is a safe place for everyone, or to operate other the UTC policies, such as the sick pay policy or equal opportunities policy, or to comply with our legal requirements to comply with Government returns. This information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students and the access to this data is limited to only those who require access to carry out these duties. As we would not be able to carry out our legal obligations without this data offers of employment or course places may be withdrawn if an individual refuses to provide this, without good reason. More information about this is available from the DPO.

12. The data controller and data processor

The UTC as a corporate body is the data controller under GDPR, and the Board is therefore ultimately responsible for implementation of all policies and processes in respect to data collection and processing. However, the designated data controllers will deal with day-to-day matters.

The UTC has two designated data controllers. They are the Principal and the Business Manager in respect of employment issues and student issues. The DPO will be the first contact in any queries regarding compliance with the GDPR.

13. Examination marks

Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide. The UTC may withhold certificates, accreditation or references in the event that all books and equipment have not been returned or debts repaid to the UTC.

14. Retention of data

The UTC will keep some forms of information for longer than others and this is laid out in the Data Retention policy.

Storage constrains mean that, information about students cannot be kept indefinitely, unless there are specific requests or legal requirements to do so. In general information about students will be kept for a maximum of five years after they leave the UTC
This will include:

- Name and address
- Academic achievements, including marks for coursework and
- Copies of any reference written.

All other information, including any information about health, race or disciplinary matters will be kept according to a schedule of retention in the retention policy.

The UTC will need to keep some information about staff for longer periods of time. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. The retention schedule can be found in the Data Retention Policy.

15. Conclusion

Compliance with the GDPR is the responsibility of all members of the UTC. Any deliberate breach of the Data Protection Policy will lead to disciplinary action being taken, or access to the UTC facilities being withdrawn, or even a criminal prosecution. Breaches of data must be reported to the ICO with 72 hours and a fine of up to £20million is possible. Any question or concerns about the interpretation or operation of this policy should be taken up with the Principal or DPO.

Appendix 1

Staff Guidelines for Data Protection

1 All staff will process data about students on a regular basis, when marking registers, or UTC work, writing reports or references, or as part of a pastoral or academic supervisory role. The UTC will ensure through registration procedures, that all students are informed of the extent and reasons for the processing of their data and are notified of the categories of processing, as required by GDPR. Staff must consider whether the reason that they are processing the data is the best and most secure way of dealing with the data. The information that staff deal with on a day to day basis will be 'standard' and will cover categories such as:

- General personal details such as name and address
- Details about class attendance, course work marks and grades and associated comments
- Notes of personal supervision, including matters about behaviour and discipline.

2 Information about staff/student's physical or mental health; sexual life; political or religious views; trade union membership or ethnicity or race is sensitive and special category data and can only be collected and processed with the staff/student's full understanding of the use of this data. If staff need to record this information, they should use the UTC standard processes. e.g: recording information about dietary needs, for religious or health reasons prior to taking students on a field trip in evolve; recording information that a student is pregnant, as part of pastoral duties. This data must be kept in accordance with GDPR requirements and a data breach of this information will be taken seriously and reported to the ICO within 72 hours.

3 All staff have a duty to make sure that they comply with the data protection principles, which are set out in the UTC Data Protection Policy. In particular, staff must ensure that records are:

- Accurate
- Up-to-date
- Fair
- Kept and disposed of securely.

4 The UTC will designate staff in each area as 'authorised staff'. These staff are the only staff authorised to hold or process data that is:

- Not standard data or
- Sensitive data.

The only exception to this will be if the DPO is satisfied that a non-authorised staff member processing of the data is necessary:

- In the best interests of the student or staff member, or a third person, or the UTC AND

- He or she has either informed the authorised the DPO of this, or has been unable to do so and processing is urgent and necessary in all the circumstances.

This should only happen in very limited circumstances. For example, a student is injured and unconscious, but in need of medical attention, e.g. a staff tutor tells the hospital that the student is pregnant or a Jehovah's witness.

5 Authorised staff will be responsible for ensuring that all data is kept securely.

6 Staff must not disclose personal data to any student, unless for normal academic or pastoral purposes, without authorisation or agreement from the data controller, or in line with the UTC policy.

7 Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated data controller, or in line with the UTC policy.

8 Before processing any personal data, all staff should consider the checklist below.

Staff Checklist for Recording Data

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the student been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, where this is required, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?
- Have you reported the fact of data collection to the authorised person within the required time?

Appendix 2: Guidelines for Retention of Personal Data

Please see the UTC Data retention policy on our website

Appendix 3. Data Protection Regulations 2018 – Privacy Statement for UTC employees

Under the General Data Protection Regulations May 2018, individuals have a right to be informed about how UTC South Durham uses any personal data that we hold about them. We comply with this right by providing a 'privacy notice' to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

UTC South Durham are the 'data controller' for the purposes of data protection law.

Our data protection officer (DPO) is:

Jean Bell who is contactable on 01325 430250 (ext 253) or via e-mail on jean.bell@utcsouthdurham.org

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Name and contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a your application form or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence
- Photographs/CCTV footage (if applicable)
- Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity
- Criminal records
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we use this data

The purpose of processing this data is to enable us run the UTC effectively, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable equalities monitoring
- Improve the management of workforce data across the sector

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

1) Carry out a task in the public interest
2) Fulfil a contract we have entered into with you
3) Comply with a legal obligation

Less commonly, we may also use personal information about you where:

4) You have given us consent to use it in a certain way
5) We need to protect your vital interests (or someone else's interests)

Where we have asked you to provide us with consent to use your data, you may withdraw this consent at any time. You may do this in writing via mail or e-mail to the DPO at UTC South Durham using the contact details above.

Some of the legal basis listed above for collecting and using personal information about you overlap, and where this occurs the legal basis will be applied in the order listed above.

Collecting this information

While the majority of information we collect from you is mandatory and allows us to carry out our legal task of educating students or fulfil our contract with you, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we will make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

Personal data is stored in line with our Data Protection Policy.

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment. Only authorised personnel have access to your file.

There is also an electronic file on the MIS which allows us to comply with Government returns and the effective running of the school and HR processes. Our contract with our MIS system ensures that they hold your data in a manner which is GDPR compliant.

Once your employment with us has ended, we will retain these file and delete the information in it in accordance with our Record Retention schedule. All sensitive data will be removed and only information that will support references, our legal obligations to HMRC or to support legal action will be retained

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law), we may share personal information about you with:

- Department for Education – we share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment of educational attainment. We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (England) Regulations 2007 and amendments
- Local Authority – we are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (England) Regulations 2007 and amendments
- Our regulator [e.g. Ofsted] – to meet our legal obligations to share certain information during the inspection process
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll
- Our auditors – to enable them to provide the service we have contracted them for
- Survey and research organisations – to enable them to provide the service we have contracted them for
- Trade unions and associations – to support you during employment processes
- Health authorities – to enable them to provide the service we have contracted them for
- Security organisations – to enable them to provide the service we have contracted them for

- Health and social welfare organisations – to meet our legal obligations to share certain information with it, such as child protection information
- Professional advisers and consultants – to enable them to provide the service we have contracted them for
- Police forces, courts, tribunals – to meet our legal obligations to share certain information with it, such as CCTV footage or contact information
- Professional bodies - to meet our legal obligations to share certain information with it, such as the Teaching Council

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law. We currently have no contracts which transfer data outside of the EEA.

Your rights

How to access personal information we hold about you

Individuals have a right to make a **'subject access request'** to gain access to the personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our DPO in writing or by e-mail.

Other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our DPO.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our DPO.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact the DPO.

Data Protection and Privacy Notice

Signed: Name: Date: