University Technical College Warrington (UTCW)

Data Protection and Educational Records Policy

Document Detail	
Reference Number	UTCW017
Category	Statutory
Authorised by	Trust Board
Author	Business & HR Manager
Version	2
Status	Approved
Issue Date	December 2017
Last Reviewed	June 2021
Next Review Date	June 2023

CONTENTS

1. COMPLIANCE

1.1. UTC Warrington (UTCW) aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the United Kingdom General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018).

1.2. This policy applies to all personal data, regardless of whether it is in paper or electronic format. It meets the requirements of the UK GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

1.3. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

1.4. In addition, this policy complies with our funding agreement and articles of association.

2. ABOUT THIS POLICY

2.1. All schools are Controllers of personal data under expected provisions of the UK GDPR and DPA 2018 together referred to as 'Data Protection Law'.

2.2. This policy sets out ~~the duties of~~how UTCW ~~under each of the legislation provisions referred to in paragraph 2 of this policy, the responsible bodies/person for compliance and the procedures that will be applied~~will comply with its obligations under Data Protection Law.

2.3. During the course of its activities UTCW will process personal data (which may be held on paper, electronically, or otherwise) about UTCW's staff (including temporary staff), agency workers, volunteers, pupils, their parents, guardians or carers, and other individuals (including suppliers and ~~governors~~trustees).

~~2.4.~~ UTCW recognises the need to treat personal data in an appropriate and lawful manner, in accordance with ~~the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the~~ Data Protection Law and associated Information Commissioner's Office

2.4. (ICO) Guidance applicable from time to time. The purpose of this policy is to make the data subject aware of how UTCW will handle personal data.

~~**2.5.** This policy also outlines the Trust Board's approach to requests made under the Freedom of Information Act 2000 (FOIA).~~

~~**2.6.** The Trust Board complies with the provisions of the FOIA which allows any member of the public to request information from public bodies including Academies created under the Academies Act 2010.~~

~~**2.7.** The Trust Board also complies with ICO and DfE Guidance applicable from time to time.~~

2.5. This policy does not form part of any employee's contract of employment and may be amended at any time.

~~**2.8.**~~

3. WHO IS RESPONSIBLE FOR THIS POLICY

3.1. The Trust Board has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework for data protection ~~and freedom of information~~.

3.2. The Trust Board has delegated day-to-day responsibility for operating the policy and ensuring its maintenance and review to the ~~UTCW Data Protection Officer (DPO) notwithstanding that UTCW is a data controller as defined in Section 1 of the DPA and public authority as defined in Section 3 of the FOIA~~Principal with advice and assistance from the DPO.

3.3. The Senior Leadership Team has a specific responsibility to ensure the fair application of this policy and all staff have an individual responsibility to ensure that they understand the implications of the data protection principles (**Principles**) outlined in paragraph 6.1.2 and that the Principles are adhered to.

4. WHO IS COVERED BY THIS POLICY

4.1. This policy covers all staff at all levels and grades including senior managers, employees, trainees, part-time and fixed term employees, permanent, temporary, agency workers and volunteers (referred to as **staff** or **data subject** in this policy).

4.2. This policy also covers how UTCW will process the personal data belonging to its students, parents, guardians and other third parties that come into contact with UTCW.

4.1.

5. DEFINITIONS

5.1. The definitions in this paragraph apply in this policy.

5.2. **Personal data:** means any recorded information UTCW holds about a living individual (data subject) from which he/she can be identified. It may include contact details, other personal information, photographs, expressionsand expressions of opinion about a data subject or indications as to UTCW's intentions about the data subject.

5.3. **Processing:** means doing almost any activity with personal data, such as accessing, disclosing, destroying or using the data in any way.

5.4. **Special Categories of personal data:** means sensitive personal data concerning a data subject's ethnic origin, political opinions, religious or similar beliefs, trade union membership, health, sex life, criminal proceedings or convictions. This personal information is deemed more sensitive and therefore needs enhanced protection.

5.5. **Data Subject**: The identified or identifiable individual whose personal data is held or processed.

5.6. **Data Controller**: A person or organisations that determines the purposes and the means of processing of personal data.

5.7. **Data Processor**: A person or other body, other than an employee of the data cController, who processes personal data on behalf of the data cController.

5.8. UTCW processes personal data relating to parents, students, staff, governors, visitors and others and therefore is a data controller. UTCW is registered as a data controlleras a fee payer with the ICO and will renew this registration annually or as otherwise legally required.

6. ROLES AND RESPONSIBILITIES

This policy applies tois applicable to **all staff** employed by UTCW, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

6.1. UTCW Trust Board

6.2. The Trust Board has overall responsibility for ensuring that UTCW complies with all relevant data protection obligations

~~6.2.~~6.3. Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with ~~data~~ Data ~~protection~~ Protection ~~law~~Law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the Trust Board and, where relevant, report to the Trust ~~b~~Board their advice and recommendations on UTCW data protection issues.

The DPO is also the first point of contact for individuals whose data the ~~school~~ UTC processes, and for the ICO. Full details of the DPO's responsibilities are set out in ~~their job description~~the UK GDPR. The DPO at UTCW is the Business Manager.

~~6.3.~~6.4. Principal ~~and Chief Executive~~

The Principal ~~and Chief Executive~~ will act as the representative of the ~~data c~~Controller on a day-to-day basis unless it involves the ICO. In such cases the DPO will engage with the ICO's case workers and representatives.

~~6.4.~~6.5. All Staff

All staff are responsible for:

~~6.4.1.~~6.5.1. ~~Collecting~~collecting, storing and processing any personal data in accordance with this policy and their training;

~~6.4.2.~~6.5.2. ~~I~~informing UTCW of any changes to their personal data, such as a change of address;

~~6.4.3.~~6.5.3. ~~Contacting~~ contacting the DPO in the following circumstances:

~~6.4.3.1.~~6.5.3.1. ~~With~~ with any questions about the operation of this policy, ~~data~~ Data ~~protection~~ Protection ~~law~~Law, retaining personal data or keeping personal data secure

~~6.4.3.2.~~6.5.3.2. ~~i~~If they have any concerns that this policy is not being followed

6.5.3.3. ~~If~~ if they are unsure whether or not they have a lawful basis to use personal data in a particular way

6.5.3.4. if they need advices for a data protection impact assessment

6.5.3.5. if a personal data breach occurs

6.5.3.6. if training is required

6.5.3.7. if new processing activities need to be added to the Trust's record of processing

6.5.3.8. If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the United Kingdom

Whenever they are engaging in a new activity that may affect the privacy rights of individuals

6.5.3.9.
6.5.3.10. If they need help with any contracts or sharing personal data with third parties.

es
6.4.3.3.

- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area

- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals

- If they need help with any contracts or sharing personal data with third parties

7. DATA PROTECTION

7.1. Data protection principles

7.1.1. Personal data' is defined in Section 1 of the DPA and is information that on its own, or in conjunction with other information UTCW's possession or likely to come into the UTCW's possession, identifies the data subject. This includes opinion.

7.1.2. UTCW will comply with the eight data protection principles in the DPA, which require that personal data must be:

7.1.2.1. processed lawfully, fairly and in a transparent manner;

7.1.2.2. processed for limited purposes the data was obtained for; and in an appropriate way;

7.1.2.3. adequate, relevant and not excessive for the purposeminimised to that which is necessary;

7.1.2.4. accurate and, where necessary, kept up to date

7.1.2.5. not kept longer than necessary for the purpose;
7.1.2.5.
7.1.2.6. processed in line with individuals' rights;

7.1.2.7.7.1.2.6. secure; and,

7.1.2.8. not transferred to people or organisations situated in countries without adequate protectionwith accountability.
7.1.2.7.

8 LAWFUL, FAIR AND TRANSPARENT PROCESSING

8.1. UTCW ~~will usually only~~rarely processes personal data where the data subject has given his/her consent. This is because it either has a legal obligation to process the personal data it collects or it is required to process it in the performance of its public task as a state funded education provider. Consent is relied upon when processing images outside of UTCW for example, on our website or in prospectus publications. For members of staff, our processing may be pursuant to a legitimate interest we have identified for the UTCW or a third party. In deciding whether to process information pursuant to a legitimate interest we will balance the interest against the rights and freedoms of the data subjects concerned.~~or where the processing is necessary to comply with the UTCW's legal obligations. In other cases, processing may be necessary for the protection of a data subject's vital interests, for the UTCW's legitimate interests or the legitimate interests of others. The full list of conditions is set out in Schedule 2 of the DPA.~~

~~**8.2.**~~ UTCW will only process sensitive personal data where a further condition is also met as set out in Schedule 1 DPA (2018). Usually this will mean that the data subject has given his/her explicit consent, ~~or that~~ the processing is legally required for employment purposes, for a substantial public interest or to establish/defend legal claims.~~s . The full list of conditions is set out in Schedule 3 of the DPA.~~

9 HOW THE COLLEGE IS LIKELY TO USE PERSONAL DATA

9.1. Staff

9.1.1. UTCW will process data about staff for legal, personnel, administrative and management purposes and to enable the college to meet its legal obligations as an employer and education provider.

9.1.2. UTCW will process personal data in order to, for example:

9.1.2.1. pay the data subject;

9.1.2.2. monitor performance;

9.1.2.3. provide information on UTCW's website in order to meet the legitimate needs of visitors to the college and enquirers looking to make contact with it;

9.1.2.4. perform recruitment and pre-employment checks;

9.1.2.5. comply with legal obligations under relevant legislation;

~~**9.1.2.5.**~~**9.1.2.6.** to comply with internal policies particularly on grievances and disciplinary matters;

~~**9.1.2.6.**~~**9.1.2.7.** confer benefits in connection with a data subject's employment.

~~**9.1.2.7.**~~**9.2.** UTCW may process sensitive personal data relating to staff including, as appropriate:

~~**9.1.2.8.**~~**9.2.1.** information about a staff member's physical or mental health or condition in order to monitor sick leave and take decisions as to the staff member's fitness for work;

~~**9.1.2.9.**~~**9.2.2.** the staff member's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation; and,

~~**9.1.2.10.**~~9.2.2.1.1. in order to comply with legal requirements and obligations to third parties.

~~9.2.~~9.3. Pupils

~~**9.2.1.**~~**9.3.1.** UTCW will process data about pupils for the following (non-exhaustive) purposes:

for legal and administrative purposes;

9.3.1.1.

~~**9.2.1.1.**~~to provide education and discharge UTCW's duty of care as an education provider;~~;~~

9.3.1.2.

~~9.2.1.2.~~ to provide pupils with a safe and secure environment and pastoral care;

9.3.1.3.

~~9.2.1.3.~~ to provide activities including school trips, activity and after-school clubs;

9.3.1.4.

~~9.2.1.4.~~ to provide academic and examination references; and,

9.3.1.5.

~~9.2.1.5.~~9.3.1.6. to enable UTCW to meet the it's legal obligations under relevant legislation and Department for Education (DfE) Guidance in force from time to time.

~~9.2.2.~~9.3.2. UTCW will process personal data in order to, for example:

~~9.2.2.1.~~ maintain educational records;

9.3.2.1.

~~9.2.2.2.~~ monitor attendance~~;~~

9.3.2.2.

~~9.2.2.3.~~ maintain health and safety records;

9.3.2.3.

~~9.2.2.4.~~ collect opinions about ability and achievements;

9.3.2.4.

~~9.2.2.5.~~ obtain and retain details about personal / home life where this is relevant to provision of education to a data subject; and,

9.3.2.5.

~~9.2.2.6.~~9.3.2.6. share information with other agencies when strictly required.

~~9.2.3.~~9.3.3. UTCW may process sensitive personal data relating to pupils including, as appropriate:

~~9.2.3.1.~~9.3.3.1. information about pupil's physical or mental health or condition (including but not limited to allergies and regular medications) in order to discharge the college's duty of care, provide non-emergency and emergency medical assistance and for special educational needs provision;

~~9.2.3.2.~~9.3.3.2. the pupil's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation or to ensure that religious or similar beliefs are respected; and/or,

~~9.2.3.3.~~9.3.3.3. in order to comply with other legal requirements and obligations to third parties.

~~9.3.~~9.4. **Parents, guardians, carers and other individuals (including suppliers and governors)**

~~9.3.1.~~ UTCW may process data about parents, guardians, carers and other individuals

(including suppliers and governors) for the purpose of:~~f.~~

~~9.3.1.1.~~9.4.1.1. providing education to pupils;

~~9.3.1.2.~~9.4.1.2. maintaining emergency contact details in order to discharge UTCW duty of care as an education provider;

~~9.3.1.3.~~9.4.1.3. organise training courses;

~~9.3.1.4.~~9.4.1.4. obtain and retain details about personal / home life where this is relevant to provision of education to pupils; and

~~9.3.1.5.~~9.4.1.5. discharge obligations under safeguarding and other relevant legislation.

~~9.3.1.6.~~9.4.1.6. It is very unlikely that UTCW will process sensitive personal data relating to parents, guardians, carers and other individuals (including suppliers and governors). However, where this may be necessary, it may include, as appropriate:

~~9.3.1.6.1.~~9.4.1.6.1. the parent, guardian, carer or other individual's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;

~~9.3.1.6.2.~~9.4.1.6.2. to comply with child protection and welfare matters, and/or,

~~9.3.1.6.3.~~9.4.1.6.3. in order to comply with other legal requirements and obligations to third parties.

10 ~~PROCESSING FOR LIMITED PURPOSES~~PURPOSE LIMITATION

10.1. UTCW will only process personal data for the specific purpose or purposes notified to data subjects or for any other purposes specifically permitted by the DPA.

10.2. If staff need to process personal data relating to volunteers, suppliers, pupils, their parents, guardians or carers, and other individuals (including suppliers and governors) outside of the original purpose for which it was acquired by UTCW, they should seek advice from the DPO.

~~**10.3.**~~ If staff are unsure about the purpose for which personal data relating to volunteers, suppliers, pupils, their parents, guardians or carers, and other individuals (including suppliers and governors) is being processed, they should seek advice from the DPO ~~Manager.~~.

11 ~~ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING~~DATA MINIMISATION

11.1. Personal data will only be processed to the extent that it is necessary for ~~the~~ a specific ~~purposes notified to the data subject~~and relevant to what task needs to be performed with the data.

12 ACCURATE DATA

12.1. UTCW will keep the personal data that the college stores about a data subject accurate and up to date. Data that is inaccurate or out of date ~~will~~ may be rectified or destroyed. Data subjects should notify UTCW if any personal details change or if the data subject becomes aware of any inaccuracies in the personal data UTCW holds about him/her.

13 ~~DATA RETENTION~~STORAGE

13.1. UTCW will not keep personal data for longer than is necessary for the purpose. This means that data will be destroyed or erased from the college's systems when it is no longer required. This will be done in line with the UTCW's Retention and Disposal Policy.

14 PROCESSING IN LINE WITH SUBJECT ACCESS RIGHTS

Data subjects have the right, under the ~~DPA~~UK GDPR, to make a 'subject access request' to gain access to personal information that the ~~school~~ College holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- For students, this also includes educational records.

Subject access requests ~~must~~ should be submitted in writing, either by letter~~,~~ or email ~~or fax~~ to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

The data requested under a subject access request may be subject to exemptions under Schedule 2 of the DPA (2018). All requests will be reviewed against applicable exemptions. If or more has been applied then this will be set out in the response provided to the requester.

14.1. Educational Record

14.1.1. UTCW is owned and operated by an academy trust. The statutory right of parents to request a copy of their child's education record does not extend to the College.

14.1.2. Any request must be treated as a subject access request and in accordance with data protection law.

~~14.1.~~14.2. **Children and subject access requests**:

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must be ~~be~~ unable to understand their rights and the implications of a subject access request, or have given their consent.

Children who have the level of understanding to know what is being asked for and how the exercising of their right of access works will be deemed to be Gillick competent and will be the only person able to determine if a subject access request can be made for their data. In England there is no prescribed age for when a child may be deemed competent. It is however generally accepted that a child will be competent enough from around the ~~aged~~ ages 12/13. From and above these ages children are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of ~~pupils~~ students at our school may not be granted without the express permission of the ~~pupil~~student. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

~~14.2.~~14.3. Responding to a subject access request

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

~~• ry~~

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child
- If the request is manifestly unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.
- A request will be deemed to be ~~unfounded or~~ excessive if it is repetitive, or asks for further copies of the same information.
- When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

15 DATA SECURITY

15.1. UTCW will ensure that appropriate technical and organisational measures are ~~taken~~ put in place against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Appropriate measures include:

15.2. Appropriate levels of authority being given to staff members where access to personal data is concerned;

15.2.1. Lockable cabinets, drawers and cupboards;

15.2.2. Laptop and other mobile device / document encryption;

15.2.3. Laptop and other mobile device / document password protection;

~~Regular back-ups of UTCW's servers;~~

15.2.4.

15.3 UTCW has procedures and technologies in place to maintain the security of all personal data from the point of collection to the point of destruction. UTCW will only transfer

personal data to a third party if he or she agrees to comply with those procedures and policies, or if he or she puts in place adequate measures himself.

~~15.5~~ 15.4 UTCW will have in place a written contract with each Processor (pursuant to Article 28 GDPR) used to carry out tasks for the Trust Board that necessitates the Processor having access to personal Processed by the UTCW.

15.5 Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.

~~15.3. r~~

~~15.4. personal data to a third party if he or she agrees to comply with those procedures and policies, or if he or she puts in place adequate measures himself.~~

~~15.5. UTCW will have in place a written contract with each data pProcessor (as defined by Section 1 of the DPApursuant to Article 28 GDPR) used to carry out tasks for the Trust Board that necessitates the data pProcessor having access to personal data pProcessed by the UTCW.~~

~~15.6. Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.~~

16 CCTV

We use CCTV in various locations around the school site to ensure it remains safe and to detect and prevent unlawful acts. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. As a state funded education provider serving vulnerable children and young people, our CCTV is in line with our public task and our wider legal obligation to safeguard children and promote their welfare. Insofar as it captures staff images, we have a legitimate interest to operate the system in allowing us to safeguard our pupils and premises.

Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the DPO. Our network of cameras are proportionate and as necessary to achieve the processing task that they are established for.

Images captured by the CCTV system may be used as evidence in criminal investigations by third parties or for internal investigations such as disciplinary, grievance and exclusion processes.

17 DATA PROTECTION BY DESIGN AND DEFAULT

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant ~~data~~ Data ~~protection~~ Protection ~~law~~ Law ~~(see section 6)~~

- Completing ~~privacy~~ data protection impact assessments where the ~~school's~~ College's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)

- Integrating data protection into internal documents including this policy, any related policies and privacy notices~~s~~

- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance

- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

- Maintaining records of our processing activities, including:

    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

18 DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

19 PERSONAL DATA BREACHES

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

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

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium

- Safeguarding information being made available to an unauthorised person

-

- The theft of a school laptop containing non-encrypted personal data about pupils

Any breach of this policy by staff will be taken seriously and may result in disciplinary action.

20 RETENTION OF DATA

20.1 UTCW will keep some forms of information for longer than others. In general information about students will be kept for a maximum of five years after they leave UTCW. This will include:

- name and address
- academic achievements, including marks for coursework and
- copies of any reference written.

20.2 All other information, including any information about health, race or disciplinary matters will be destroyed within three years of the course ending and the student leaving UTCW.

20.3 If students leave the UTC at 16 to study at another school or college, their personal files and online CTF files will be sent via secure access to their new school or college.

20.4 UTCW will need to keep information about staff for longer periods of time. In general, all information will be kept for six years after a member of staff leave. Some information however will be kept for much longer. 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. A full list of retention periods are shown in Appendix 2 – UTW Data Retention Schedule.

~~Any breach of this policy by staff will be taken seriously and may result in disciplinary action.~~

21 TRAINING

All staff and ~~governors~~ trustees are provided with data protection training as part of their induction process.
Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

22 PROVIDING INFORMATION TO THIRD PARTIES

a. UTCW will not disclose personal data to a third party without the data subject's consent unless UTCW is satisfied that they are legally entitled to share the data. Where the UTCW does disclose personal data to a third party, the UTCW will have regard to the ~~eight data protection~~ principles set out under Article 5 UK GDPR.

b. If staff receive a request from a third party for personal data, or consider that they need to disclose personal data to a third party, they should seek advice from the DPO unless it is something which has previously been agreed or common practice in the circumstances. This may include (but is not limited to) requests from parents, or other members of staff, for personal data relating to other members of staff (including temporary staff), agency workers, volunteers, suppliers, pupils, their parents, guardians or carers, and other individuals (including suppliers and governors). It will also include requests to share information with the Local Authority, Police or Department for Education.

c. Any member of staff who knowingly or recklessly, without the Trust Board's consent, obtains or discloses personal data or procures the disclosure to another person, commits an offence under Section ~~55~~ 170 of the DPA (2018) and may be subject to disciplinary proceedings under the Trust Board's Disciplinary Policy.

d. The DPA (2018) also creates offences in relation to data protection as follows:

i. section 173 – altering, defacing, blocking or erasing personal data in order to prevent disclosure following a request for access by a data subject; and

ii. ~~section~~Section[TF1] 171 – re-identification of information which has been anonymised.

~~19.1.~~ If either of the offences under sections 173 or 171 appear to have been committed they may be subject to criminal investigation and UTCW's disciplinary procedures (as ~~-~~appropriate)~~.~~

~~20 PUBLICATION SCHEME~~

~~**20.1.** The Trust Board understands its duties under the FOIA to be transparent and proactive in relation to the information that it makes public.~~

~~**20.2.** The Trust Board has adopted the DfE's Model Publication Scheme for Academies and this is available on the UTCW's website.~~

~~**21** REQUESTS~~

~~**21.1.** The FOIA applies to all recorded information held by the Trust Board, along with information held by a third party organisation on behalf of the Trust Board.~~

21.2. Any member of staff that receives a freedom of information request (or believes that they may have done so) should forward it without delay to the DPO. The Trust Board has a statutory timeframe to adhere to which is 20 working days, and failure to promptly report a freedom of information request (or a request believed to be a freedom of information request) may lead to disciplinary action.

21.3. The Trust Board will provide a response to a freedom of information request within 20 working days unless the data subject is notified that the statutory timeframe is extended by a necessity to consider the public interest test.

22 ADVICE AND ASSISTANCE

22.1. The DPO, on behalf of The Trust Board will provide advice and assistance to requesters in accordance with Section 16 of the FOIA**.**

23 Internal review

23.1. The Trust Board operates an internal review procedure for any requester that is dissatisfied with the handling of their freedom of information request by the UTCW. Internal reviews will be carried out by a senior member of staff who has not been involved in making the original decision or responding to the request.

23.2. As part of the UTCW's internal review procedure, the Trust Board will consider whether or not the request was handled appropriately and in accordance with the requirements of the FOIA.

23.3. Requesters seeking an internal review must write to the DPO within 40 working days of the date of UTCW's response to the original request stating the grounds for the review.

23.4. UTCW will endeavour to respond to requests for internal review within 20 calendar days of receipt of the request. Where this is not possible, UTCW will write to the requester to inform them of the expected date of response to their request for internal review.

23.5. Requesters who are unhappy with the outcome of the internal review may raise a complaint with the ICO.

24 MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy.
This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill

~~that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the Trust Board.~~

APPENDIX 1 - PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the Principal ~~and Chief Executive~~ and the Chair of the Trust Board.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss

- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

- If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are held by the DPO and stored on UTCW's computerised system.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

    - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

- Records of all breaches will be held by the DPO stored on UTCW's computer system.
- The DPO and Principal ~~and Chief Executive~~ will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*

- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*

- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it*

- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*

- *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*

- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

Other types of breach that you might want to consider could include:

- *Details of pupil premium interventions for named children being published on the school website*
- *Non-anonymised pupil exam results or staff pay information being shared with governors*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked*
- *The school's cashless payment provider being hacked and parents' financial details stolen*

~~n.~~

Appendix 2 - UTCW Data Retention Schedule

Data Source	Type of Data	Retention Period
Student data Student data (MIS)	Student files saved on MIS system (sent securely via online database)	5 years
Student data Personal data	Name and address Academic achievements and copies of any reference written. Health, Race, Disciplinary matters	5 years 3 years
Student data Safeguarding information	Safeguarding reports/ case minutes	5 years
Student data SEND Information	SEND Reports/intervention logs	35 years after closure of file
Student data Attendance Registers	Attendance register	3 years from completion
Governance Policies	All policies	Policies – until no longer operational
Governance Trustee Records	Trustee personal records / companies house resolutions	6 years for signed version
Governance Minutes	Signed minutes of Trust Board meetings	6 years for signed version
Governance Complaint files	Complaint letters/logs and outcomes	6 years - Complaint files
Management Minutes of meetings	Minutes of management meetings	5 years from date of meeting
Management School development plan		3 years
Statutory returns Census		5 years
Statutory returns ESFA Returns		ESFA Returns – 10 years
Payroll Income Tax and NI returns, including correspondence with tax office		At least 3 years after the end of the financial year to which the records relate
Payroll Statutory Maternity Pay records and calculations		At least 3 years after the end of the financial year to which the records relate
Payroll Statutory Sick Pay records and calculations		At least 3 years after the end of the financial year to

		which the records relate
Payroll Wages and salary records		6 years
Health and Safety Accident books, and records and reports of accidents		3 years after the date of the last entry
Health and Safety Medical Records	kept by reason of the Control of Substances Hazardous to Health Regulations 1994	40 years
Financial Information Annual Accounts		6 years
Personnel Files Employee files		6 years from the end of employment
Personnel Files References		6 years from the end of employment
Personnel Files Application forms		At least 6 months from the date of the interviews.
Personnel Files Redundancy records	Facts relating to redundancies where less than 20 redundancies	3 years from the date of redundancy
Personnel Files Redundancy records	Facts relating to redundancies where 20 or more redundancies	12 years from date of redundancies
Personnel Files Health records	General Health questionnaire	During employment
Personnel Files Health records	Where reason for termination of employment is connected with health, including stress related illness.	3 years

NAME:

JOB TITLE:

I confirm I have received a copy of the UTC Warrington Data Protection policy and that I have read and understood the contents.

~~I agree complete mandatory Data Protection training via Flick Learning.~~
I confirm that if I need clarification on any matter outlined in the Data Protection policy, or if I am unsure whether a data breach has occurred, I will approach the Data Protection Officer (Miss M Ward).

Signed:_____
Date: _____

Please return the completed form to the Business Manager ~~'s office (room 5.27)~~