DATA PROTECTION
POLICY & PROCEDURE

Ref No	0001	**Version**	1.6
Dept	College Wide	**Last Updated**	1 May 2024
Responsible Manager	Vice Principal Finance & Resources	**Next Review**	1 May 2026
Date Approved	8 July 2024	**Category**	Public
Where Approved	Corporation	**Covers**	Staff/Students
Equality Impact Assessment Completed		Yes	

Contents

Introduction

Telford College is committed to preserving the privacy of its learners and employees and to complying with the Data Protection Act 2018 (DPA) & UK GPDR. To achieve this commitment, information about our learners, employees and other clients and contacts must be collected, used fairly, stored safely and not unlawfully disclosed to any other individual or organisation.

It is college policy and mandatory for confidential information in digital form to be protected using encryption where it is taken or sent out of a physically secure college location. Within the college environment all reasonable physical security precautions must also be taken.

Information that is already in the public domain is exempt from the Data Protection Act 2018 & UK GDPR. It is the College's policy to make as much information public as possible. Information already available to the public can be found under Governance on the College website (https://www.telfordcollege.ac.uk/governance/)

Scope

The College needs to process certain personal data about employees, learners and third parties in order to monitor performance, achievements, fulfil its purpose and to meet its legal obligations to funding bodies and the government. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. Any personal information must be collected and dealt with appropriately whether it is collected on paper, entered electronically or stored in a computer database. All Telford College information is categorised into two main classifications:

- Public
- Confidential

The College must comply with the Data Protection Principles as set out in the Data Protection Act. In summary the principles state that information should be:

- Be obtained and processed fairly and lawfully
- 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 be kept longer than is necessary for that purpose
- Be processed in accordance with the data subject rights
- Be kept safe from unauthorised access, accidental loss or destruction
- If data is transferred outside of the European Economic Area (EEA), all controls and data protection laws are adhered to and authorisation is obtained.

The College will not release staff or student data to third parties except to relevant statutory bodies or where the relevant Third Party Processing Agreement is in place. In all other circumstances the College will obtain the consent of the individuals concerned before releasing personal data.

In many parts of the college, basic physical security of offices and the information stored therein is determined by the staff who work in those offices. Staff are therefore expected to take reasonable steps to physically secure confidential information held within offices.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

This policy is published on the College website and is subject to an bi-annual review.

Data Controller and College responsibilities

The Corporation board is responsible for the oversight and implementation of this policy.

It will be the responsibility of the Principal & Chief Executive and the Senior Leadership Team to ensure compliance with the policy and for communicating the policy to all staff.

The College's designated Data Controller is the Head of MIS & Exams who has the strategic & operational responsibility, on behalf of the college to ensure:

- The College's Policy and Codes of Practice are appropriate for the types of personal data being processed
- The College maintains an up-to-date notification of its use of personal data with the Data Protection Commissioner
- The Data Controller determines the purposes and the manner in which personal data is to be processed.

The Head of MIS & Exam is supported in their duties by the Senior Information Risk Officer. The Head of MIS & Exams who is the Data Protection Officer manage the day-to-day data protection requests and queries.

There are other designated managers within the College's organisational structure that have specialist areas of responsibility that are subject to requirements of the Data Protection Act (DPA):

- All members of the College Executive and Leadership Team
- Head of MIS & Exams
- Director of IT & Digital Innovation
- Curriculum Directors
- Assistant Principal Student Experience and Safeguarding

Any enquiries with regard to the DPA should be addressed initially to the Data Protection Officer (dpo@telfordcollege.ac.uk). The Head of MIS & Exams / Data Protection Officer manage and monitor all data protection enquiries through a centralised system to ensure the responsibilities of the college are met.

All staff are responsible for ensuring that:

- They have read and are familiar with the College Data Protection policy & procedures
- All personal data provided to the college is accurate and up to date
- They have participated in the mandatory Data Protection Act 2018 and UK GDPR Data Protection training
- Personal data they hold is kept securely and transported safely as approved by the Data Protection Officer
- Personal data is not disclosed in any way or to any unauthorised third party

This policy does not form part of the formal staff contract of employment, but it is a condition of employment that staff abide by the rules and policies made by the College. Any breach of the policy could, therefore, result in disciplinary proceedings. It may also result in a personal liability for the individual staff member.

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 Protection Officer, who will investigate further. If the issue remains unresolved then it is escalated following the escalation procedure.

Student Obligations

Students must ensure that all personal data provided to the college is accurate and up to date. They must ensure that changes to their personal details (e.g. address/contact details) are updated with the management information team.

Students who use the college computer facilities may, from time to time, process personal data. **If students collect any personal data it should be used for college work only and kept secure at all times.**

Notification of Data Held & Rights of Access

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

- What information the College holds and processes about them and why
- How to gain access to it
- How to keep it up to date
- What the College is doing to comply with its obligations under the Data Protection Act 2018 & UK GDPR

Staff, students and other users of Telford College have the right to access any personal data that is held about them either electronic or paper based. Any person who wishes to exercise this right must complete the college's Subject Access Request Form and send it to the college's Data Protection Officer at the email address given on the form **(Appendix 2).**

The College will aim to comply with requests for personal data within one calendar month.

Sensitive Information

It is understood that some information is more sensitive and is protected in a more secure manner such as student and staff personal information i.e. name, address details, contact details, safeguarding information, and any other information which identifies a person and so deemed confidential. Also included but not deemed critical data are telephone directories, external company information, address, etc., which does not require as stringent a degree of protection.

A subset of Confidential information is "Third Party Confidential" information. This is confidential information belonging or pertaining to other companies (organisations) that are stored on the College's CRM systems and databases or in paper format which has been entrusted by that company under non-disclosure agreements and other contracts. Examples are information from joint development efforts to vendor lists, customer orders, and supplier information which ranges from extremely sensitive to information regarding the College's connection to a supplier / vendor and network to support our operations.

Telford College employees are encouraged to use common sense judgment in securing confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, they should contact their line manager, or the Data Protection Officer for further advice.

The Sensitive Information: Terms, Definitions and Guidance **(Appendix 3)** provides further detail on how to protect information at varying sensitivity levels. These guidelines are set out to assist the reader to assess the level of confidentiality of the information depending upon the circumstances and the nature of the information.

Subject Consent

In many cases, Telford College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, explicit consent must be obtained which would include a mandatory identity check.

Agreement to the college processing some specified classes of personal data is a condition of acceptance of an individual onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.
Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. Telford College has a duty under the Children Act and other legislation to ensure that staff are suitable for any job offered.

The college also has a duty of care to all staff and students and must therefore make sure that employees and those who use the college's facilities have been through suitable eligibility checks to ensure safety of staff and students is maintained.

The College will also ask for information about particular health needs and disabilities. The college 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.

All prospective staff and students will be asked to sign the appropriate staff recruitment or student enrolment form to collect information when offered employment or course study. A refusal to sign such documents may result in the offer being withdrawn.

Transfer of Information to Data Processors and Contractors

Any third party or contractor who has access to Telford College's obtained personal data and/or is acting as data processor should be fully aware of their obligations to comply with the Data Protection Act, be registered with the ICO and be contracted to act accordingly using the College's Third Party Processing Agreement. This includes any contractor who is accessing areas where obtained personal data is stored or can be viewed/accessed.

No data will be transferred or made available to any party unless a Data Sharing Agreement is completed and registered with the Data Protection Coordinator in advance.

Data Protection Laws impose strict controls on Personal Data being transferred outside the UK-GDPR. Transfer includes sending Personal Data outside the UK-GDPR but also includes storage of Personal Data or access to it outside the UK-GDPR. It needs to be thought about whenever the College appoints a supplier outside the UK-GDPR or the College appoints a supplier with group companies outside the UK-GDPR which may give access to the Personal Data to staff outside the UK-GDPR. Any transfers outside of the UK-GDPR must be approved by a senior member of staff.

Student Reference Requests

Reference requests may be sought form external organsiations in relation to students attending the College. The Data Protection Policy sets out detailed guidance at Appendix 2 of the responsibility and duty in providing a student reference.

Please note that this guidance applies to all Telford College staff and representatives, (including employees, temporary staff, visiting faculty and or contractors). This guidance uses the term "staff" but applies to anyone giving a reference for a student as a result of their role at Telford College or their relationship with the student.

Retention of Data

Data will be retained subject to the explicit data retention period as per the College's Retention Policy document and in accordance with our legal responsibilities.

Conclusion

Compliance with the Data Protection Act 2018 and UK GDPR 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 directed to the Data Controller.

Data Privacy Notice

This Privacy Policy explains what happens to any personal data that you provide to us, or that we collect from you whilst you visit our site.

We do update this policy from time to time so please do review this policy regularly.

Telford College is what's known as 'the controller' of the personal data you provide to us. We need to know your basic personal data in order to provide you with details regarding your interaction with the College, it will also be used by the college's analysis services, where appropriate. We will not collect any personal data from you that we do not need in order to provide and oversee services to yourself.

We have a Data Protection regime in place to oversee the effective and secure processing of your personal data. We shall not disclose the information you entrust us with to third parties except where we have a statutory or contractual duty to do so (including to your employer, if sponsored), where you have given prior approval or where an official third party data sharing agreement exists.

Telford College will use your name and email address to inform you of our future offers and similar products or services. This information is not shared with third parties and you can unsubscribe at any time via phone, email or on our website.

More information regarding Telford College's data protection policy can be found on our website.

Under the current Data Protection Act 2018 and UK GDPR the Information Commissioner's Office Privacy Notices Code of Practice, privacy notices should be on all collection points where personal data is being collected from a Data Subject, especially if the data is being collected for a new purpose.

Your Personal Data:

What we need
Telford College will be what's known as 'the controller' of the personal data you provide to us. We only collect basic personal data about you which does not include any special or sensitive types of information. This does however include your name, address, email etc.

Why we need it
We need to know your basic personal data in order to provide you with details regarding your interaction with the college and analysis services in line with this overall contact. We will not collect any personal data from you that we do not need in order to provide and oversee any services to yourself.

What we do with it
All of the personal data we collect is processed by our staff in the UK however for the purposes of IT hosting and maintenance this information may be located on servers within the European Union. No third parties have access to your personal data unless UK law allows them to do so or an official processing agreement is in place with Telford College. We have a Data Protection regime in place to oversee the effective and secure processing of your personal data. More information on this framework can be found on our website.

How long we keep it
We are required under UK tax law to keep your basic personal data (name, address, contact details) for a minimum of 6 years (plus current year) after which time it will be destroyed. Your information that we use for marketing purposes will be kept until you notify us that you no longer wish to receive this type of information.

What we would also like to do with it
Telford College would however like to use your name and email address to inform you of our future offers and similar products. This information is not shared with third parties and you can unsubscribe at any time via phone, email or on our website.

What are your rights?

Your right to access
You have the right to ask us for copies of your personal information. This right always applies. There are some exemptions, which means you may not always receive all the information we process.

Your right to rectification
You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete. This right always applies.

Your right to erasure
You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing
You have the right to ask us to restrict the processing of your information in certain circumstances.

Your right to object to processing
You have the right to object to processing if we are able to process your information because the process forms part of our public tasks, or is in our legitimate interests.

Your right to data portability
This only applies to information you have given us. You have the right to ask that we transfer the information you gave us from one organisation to another, or give it to you. The right only applies if we are processing information based on your consent or under, or in talks about entering into a contract and the processing is automated.

Rights related to automated decision making including profiling
You have the right to not be subject to a decision based solely on automated processing. Processing is "automated" where it is carried out without human intervention and where it produces legal effects or significantly affects you. Automated processing includes profiling.

You are not required to pay any charge for exercising your rights. We have one calendar month to respond to you.

If at any point you believe the information we process on you is incorrect, and you wish to raise a complaint on how we have handled your personal data by contacting the Data Protection Officer at email address dpo@telfordcollege.ac.uk outlining your specific requirements.

If you are not satisfied with our response or believe we are processing your personal data not in accordance with the law you can escalate your complaint by following the College's escalation process.

For more information about your rights please refer to the ICO website. https://ico.org.uk/your-data-matters/

Information We Collect

In running and maintaining our website we may collect and process the following data about you:

- Information about your use of our site including details of your visits such as pages viewed and the resources that you access. Such information includes traffic data, location data and other communication data.
- Information provided voluntarily by you. For example, when you submit an application.
- Information that you provide when you communicate with us by any means.

Data Protection Compliance

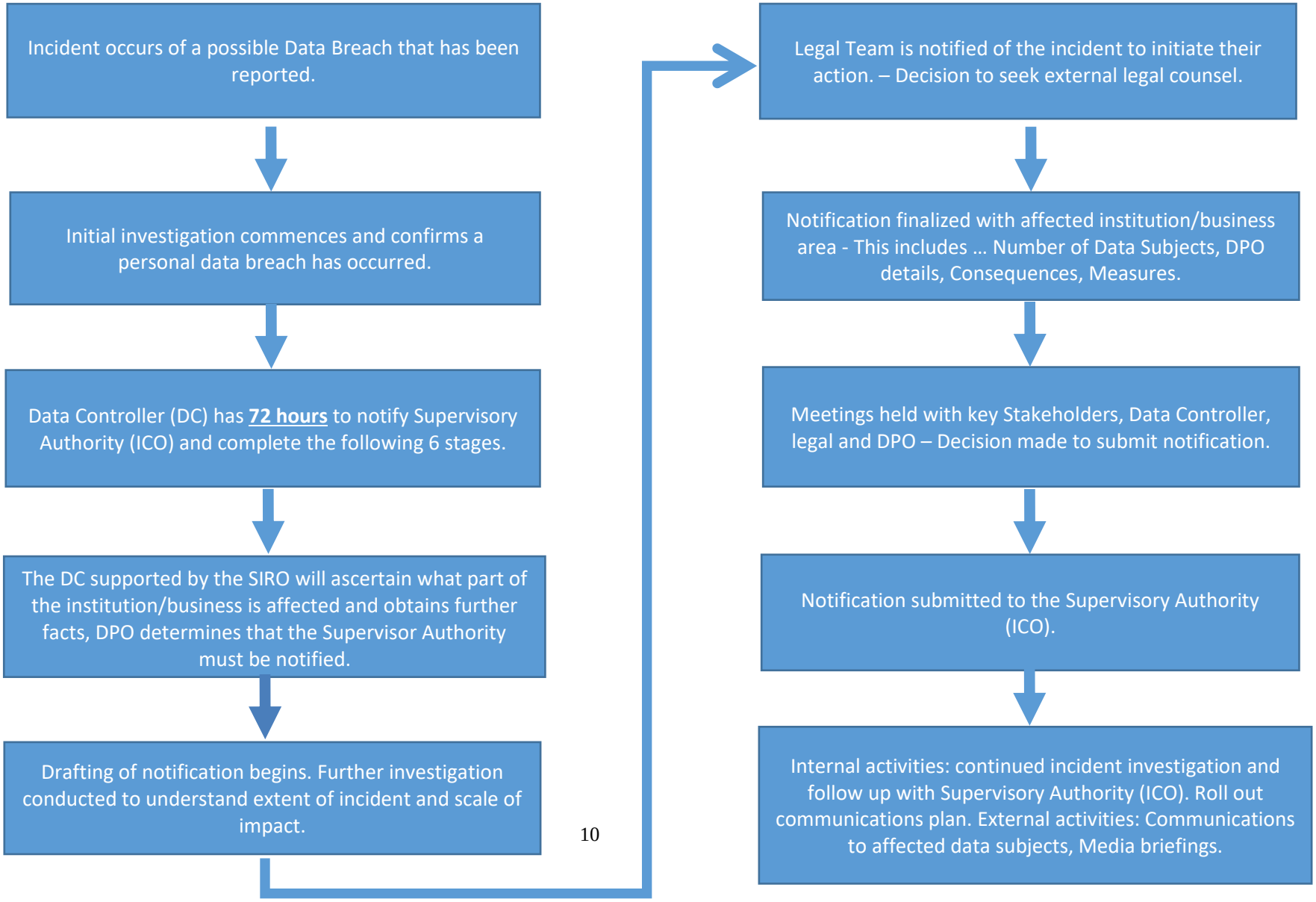
The college will be required to follow several new obligations for securing and protecting student and employee data through the General Data Protection Regulation (UK GDPR). The college is required to comply with the Data Protection Act 2018 and the regulations in the UK GDPR.

UK GDPR Fines imposed by the ICO after a serious data breach

The **UK GDPR** and DPA 2018 set a maximum **fine** of £17.5 million or 4% of annual global turnover – whichever is greater – for infringements.

The Colleges Data Breach Process

In the event of a data breach occurring, the following diagram sets out the process to follow to ensure the College remains within ICO guidelines of ascertaining evidence, assessing the severity of the breach and managing the reporting process.



Appendix 1 – Subject Access Request Form

Under the terms of the Data Protection Act 2018 and UK GDPR, staff, students and other users of Telford College, have the right to access personal data relating to themselves that is held by the college in electronic and/or manual records that form part of a 'relevant filing system'.

Any individual who wishes to exercise this right should apply using this subject access request form in the first instance.

Telford College needs to be assured of an applicant's identity and due diligence will be performed prior to any data being released. There will be no fee when a request for the release of data is made. Data will, where possible, be supplied in PDF format via email to the address provided below.

The college may hold personal records in different parts of its organisation, to assist us to supply the information you require, please provide the following information:

Details
Surname: Former Surname (if applicable): Forename(s): Date of Birth: Address: Postcode: Telephone Number: Email address:

Learner
Are you a past or present learner of Telford College, Telford College of Arts & Technology or New College Telford? Give details of your course of study and dates attended:

Staff
Are you a past or present member of staff? College and department: Dates employed:

Other
If not staff or learner, please detail the connection with Telford College and the reason for your request:

Information Required
Telford College may hold your personal records in different parts of the organisation. Please specify the information you require in order to assist us to expedite your request. Examples of data kept are (please tick as appropriate or provide full details of your request) ☐ Academic marks or course work details ☐ Academic or employment references ☐ Student Reports ☐ Disciplinary records ☐ Health and medical matters ☐ Political, religious or Trades Union information ☐ Any statements of opinion about my abilities or performance ☐ Personal details including name, address, date of birth etc. ☐ All the data that Telford College currently has about me, either as part of an automated system or part of a relevant filing system Information Required:

Signature:

Date:

On completion please send this form along with any supporting documentation to:
Email: dpo@telfordcollege.ac.uk

Post: FAO the Data Protection Officer, Telford College, Haybridge Road, Wellington, Telford, TF1 2NP

College Use Only
Reference Number: Date Received: Details of Identity Confirmed:

Appendix 2 - Student Reference Requests

1 Purpose

This procedure gives guidance to teaching staff and explains their responsibilities and legal liabilities when providing references on behalf of existing or former students.

This document also refers to the 'Student Reference Subject Access Data Request Process flow to third parties i.e. Employment Agencies, Screening Companies, Organisations and or any other institutions' – Flow diagram.

2 Policy and Procedures Statement

2.1 Telford College will, where possible, provide confidential references for current and former students.

3 Scope

3.1 The policy and procedures apply to students, screening companies and employment agencies including potential employers and or other institutions (third parties) seeking references from Telford College.

3.2 While there is no legal obligation on the College to provide a reference to a third party that is external to the College, It is the staff member's your decision whether to give a reference, or not the College recognises that it has to treat students fairly and will provide references were possible.

3.3 Normally the College is asked to provide references for students for employment purposes. However, references may be provided for other purposes, for in support of university entrance, a mortgage application or when renting accommodation. The principles outlined in this policy applies to all references.

4 Responsibilities

4.1 The Data Protection Officer is responsible for the management of this policy.

4.2 Curriculum Managers and the Assistant Principal Student Experience and Safeguarding and teaching staff are responsible for ensuring they comply with this policy. Referees have a responsibility to be truthful, not to be malicious and to include only what is accurate, true, fair and reasonable.

4.3 Teaching staff have the responsibility to ensure that any student references are prepared in accordance with the policy, and to sign the references.

4.4 The college is not obliged to give out a detailed reference if the appropriate Curriculum Manager and the Assistant Principal Student Experience and Safeguarding feels that it's not appropriate to do so.

4.5 The responsibility of obtaining consent and an identity check to grant the reference, is the responsibility of the appropriate Curriculum Manager and the Assistant Principal Student Experience and Safeguarding. This includes managing the reference from the teaching staff and or learner service staff involved and from the third party.

4.6 Consent and identity check from the student from the college is required before commencing with the reference request from the third party. If consent and identity check cannot be obtained the reference request is declined.

(i). Please note that not acquiring consent and performing a valid identity check from the Student (current/previous) would put the college under risk of an investigation from the ICO (Information Commissioners Office) for if a student's PII (Personal Identifiable Information) data was acquired by deception. The college would be liable and would incur a fine and possible criminal prosecution for the staff member involved in processing the data request.

4.7 Consent from the student submitted by the third party is not acceptable. The college initially initiates an identity check and consent to the student otherwise the reference is denied as referenced by clauses 4.5, 4.6.

4.8 Reference requests received from any organisations or institution for a student are completed within one calendar month from receipt of consent from the student.

4.9 Oral references have the same legal standing as written references and, therefore, must not be given.

4.10 Reference requests received from the third party that require you to complete the reference online via embedded web links in an email are prohibited due to the possibility of phishing (student information gained by deception by an unauthorised third party). If the member of staff is unsure when receiving an email of this type on whether to click on the web email link or not, then please contact the Data Protection Officer who will provide advice on how to proceed.

4.11 Reference requests from the third party are completed by the third parties proforma documents only and sent once completed as an attached encrypted file by email to the third party.

4.12 The responsibility is with the Curriculum Managers and Assistant Principal Student Experience and Safeguarding when recording consent and forwarding on the evidence of completed references outlined in clause 6.7.1 to the reference@telfordcollege.ac.uk mailbox by following paragraph 3 of the '*Guidance on obtaining student consent and releasing sensitive information about a student*.'

5 General Principles

5.1 Existing and former students should obtain in writing the permission of the member of staff they nominate as a referee.

5.2 References written by a member of teaching staff shall be available on request to the individual concerned.

5.3 All references shall be signed by the relevant member of the teaching staff.

5.4 Under no circumstances will reference contain any information regarding Disclosure under Part V of the Police Act 1997. http://www.legislation.gov.uk/ukpga/1997/50/part/V

5.5 Personal references should not be provided.

6 Procedures – When to give references

6.1 All requests for references must be submitted in writing which can include email and or by letter.

6.1.1 Detailed references shall typically only be given for students who have studied or are studying on a full-time or other substantial courses of study.

6.1.2 Consent and valid identity check from the student is required before the reference is completed otherwise the reference is denied as referenced by clauses 4.5, 4.6. Please be aware that consent and identity check has to be a valid email that has been cross checked from the enrolment database for it to be a valid request.

6.1.3 Detailed references for former students will typically be given within two years after leaving the College.

6.1.4 When a reference is requested for a student who has been away from College for more than two years this will generally be restricted to an attendance and achievement record only.

6.1.5 All completed references sent from the college to an organisation and or third-party will need to be sent as an encrypted file.

(i). Please note that it up to the discretion of the sender sending the reference on whether it is required to be encrypted or not. Any email sent as an unencrypted file containing student PII (Personal Identifiable Information) to an incorrect third party would result in an external data breach. Please also be aware that it would put the college under risk of an investigation from the ICO (Information Commissioners Office) and the college would be liable and would incur a fine and or criminal prosecution for the staff member involved in processing the data request.

6.1.6 Data Protection Log for auditing purposes - Send a copy in one email to reference@telfordcollege.ac.uk of the initial reference request from the requestor (third party), the consent email from the student and the completed reference email sent with the attached encrypted files and password to decrypt it.

7 Format

7.1 References must be given in writing and meet the requirements as specified in these procedures.

7.2 Oral references have the same legal standing as written references and, therefore, must not be given.

7.3 All references (written or verbal) must contain the disclaimer set out at paragraph 18.

8 Providing References for existing or former Students

8.1 References should generally be given in confidence to the third party requesting the reference. Although reference subjects have no automatic right to see what is being written about them, although they may gain access to the reference by requesting the information.

8.2 In providing a reference, both the College and referee accept certain responsibilities and liabilities. In addition to data protection subject access rights (see College's Data Protection Policy above), documents may have to be disclosed in connection with litigation.

9 Defamation

9.1 A reference must not contain a false or unsubstantiated statement which damages the reputation of the individual.

10 Deceit

10.1 reference must not contain a false statement which is made with the intention that the person receiving the reference will act on the false information.

11 Negligence and the Duty of Care

11.1 The person giving the reference must ensure that all facts included within the reference have been checked, and that reasonable care has been taken in the preparation of the reference.

11.2 The College has a duty of care to its students (both current and past) and to third parties to whom it supplies references. This duty of care requires that references are provided in good faith and are fair, reasonable, true and accurate as well as not being misleading when considered overall. This may mean that the person preparing the reference does not knowingly omit facts from the reference.

11.3 If there is an issue arising out of clause 11.2 the referee should advise the student (or former student) that information may be provided which could prove detrimental to their application.

12 Who may provide references on behalf of Telford College

12.1 Teaching staff may provide references for students on behalf of Telford College. However, because of the above legal implications, student references should/can be scrutinised by the relevant Curriculum Managers and Assistant Principal Student Experience and Safeguarding as confirming compliance with this procedure.

13 Contents of References

13.1 The referee has to disclose only that information which is relevant to the post for which the application refers, e.g. University entrance, employment etc.

13.2 The two principal aims of a reference are to confirm facts and to provide an opinion as to suitability based on an assessment of performance as a student, for example, their attendance, and the standard of work.

13.3 A reference relies on both fact and opinion and it is essential to differentiate between the two. It must in all cases be accurate, reasonable, not mislead and give a fair overall impression of the student concerned.

13.4 Factual information should be able to be substantiated.

13.5 Subjective opinions on suitability must be avoided.

13.6 The style of the reference should be clear, unambiguous and not malicious in any way.

13.7 Copies of all references should be retained by the referee and a copy sent to reference@telfordcollege.ac.uk with the password to decrypt it outlined in clause 6.1.6.

13.8 On occasion a reference will be requested using a proforma issued by the third party. The proforma, when completed must contain a covering email/letter including the disclaimer as outlined in clause 18.1.

14 Disclosure of Information

14.1 The College owes a duty of confidentiality in respect of specific information which it holds about its students and has an obligation under the Data Protection Act 2018 and UK GDPR to process data fairly and lawfully.

14.2 Referees should not include extraneous information, and they should not refer to misleading and or by withholding information because it may be damaging to the student's prospects.

14.3 Student Safeguarding information is prohibited in references as outlined in 'Appendix 4 – The disclosure of student Safeguarding information'.

15 Disciplinary Record

15.1 Statements in a reference should not refer to complaints or to difficulties that have not been raised with the student concerned.

15.2 Where a disciplinary warning is outstanding it may be referred to if relevant to the post for which the student has applied. However, a pending investigation where no disciplinary action has been taken should not be referred to in writing. There may be exceptions, for example, if the alleged disciplinary offence is one of exclusion or gross misconduct.

16 Health

16.1 Information concerning a student's physical or mental health is likely to be classified as confidential and sensitive personal information in terms of the Data Protection Act 2018 and UK GDPR as special category data (*Please refer to 'Guidance on obtaining student consent and releasing sensitive information about a student' and Appendix 4 - The disclosure of student Safeguarding information.).*

17 Dismissal

17.1 A referee must not provide a favourable reference for a student expelled from the College.

18 Disclaimer

18.1 All references will contain the following disclaimer
"This reference, prepared by [*insert name of College referee*] is provided in good faith based upon current information known to me about [*insert Student Name*] and without any liability being accepted for omissions".

19 Data Protection Act 2018 & UK GDPR

19.1 Since 25th May 2018, students are entitled under this Act to make a "subject access request" for personal data held about them in the College's appropriate electronic and or paper based filing systems. The College will allow students to view any references retained by the College.

20 Complaints

20.1 If a referee receives a complaint about a reference, the matter referred to the Data Protection Officer.

Guidance on obtaining student consent and releasing sensitive information about a student

It is our obligation to ensure that that students give consent in writing before we provide reference. This is because we will be providing their personal information, and possibly sensitive personal information, to the organisation (third party), referred to the policy in the above section 3.1 when completing the reference.

If a member of staff receives a request directly from a screening company, employment agency, potential employer, contact is to be made with the student to check that they are in agreement to you providing the reference. Although unlikely, the request may not be genuine and may be an attempt to obtain information under false pretences.

A copy of all consents must be kept on file and forward the evidence of consent including a copy of the reference email sent including attached encrypted file (and password to decrypt the attachment) to reference@telfordcollege.ac.uk outlined in more detail in clause 6.1.6 It may be that consent will apply to more than one reference (if the student is applying for several roles, or if they re-apply having been unsuccessful). To rely on a previous consent when receiving a new request, you would also have to consider whether the reference raised any different issues that would need specific consent (e.g. if the form asked many more questions about potentially sensitive matters).

Sensitive personal information – Special category data as covered in the Data Protection Act 2018 and UK GDPR. Any data listed in the below bullet points will need to be forwarded onto the Data Protection Officer before obtaining explicit consent of the student please note that this is further explained in **Appendix 4 –The disclosure of student Safeguarding information**,for if you are going to disclose any sensitive personal information in a reference.

Sensitive personal information is information about:

- racial or ethnic origin;
- political opinions;
- religious beliefs (or beliefs of a similar nature or non-belief);
- trade union activities;
- genetic data;
- biometric data (where used for identification purposes);
- physical or mental health (including any disability) or responsibilities caring for others with a disability;
- sexual life including orientation;
- criminal offences;
- age;
- gender reassignment;
- pregnancy and maternity; and
- marriage or civil partnership.

Appendix 3 – Sensitive Information: Terms, Definitions & Guidance

The following sets out terms and definitions associated with sensitive information:

Examples of Sensitive information
Includes, but not limited to:

- information critical to the business continuity of the College,
- Sensitive college financial and business information.
- Exam questions (refer to the Examinations Office instructions).
- Confidential internal documents.
- research data subject to contractual non-disclosure agreements and information held in business-critical applications.

Processing
Includes the sending of information via email, other mechanisms and any operation on data such as but not limited to organisation, adaptation and alteration; retrieval, consultation or use; disclosure, transmission, dissemination and otherwise making available; or alignment, combination, blocking, erasure and destruction.

Guidance for Information Security
Always use the College's central and secure shared drives to store and access personal data and sensitive information which belongs to the College;

At all times, use the Colleges Microsoft 365 cloud-based encrypted storage area for College business. Do not:

- Use third-party hosting services for college business that have not been authorised for College use, for example Dropbox or Google Drive.
- View high risk personal data or sensitive information in public places. When accessing your email remotely, exercise caution to ensure that you do not download unencrypted high risk personal data or sensitive information to an insecure device. Use physical security for high-risk personal data or sensitive information at all times.
- Send high risk personal data or sensitive information by email or using email to store such information without encryption.
- keep personal data and sensitive information that you do not need. In identifying master copies of records, staff should seek advice from IT Helpdesk for encryption keys, e.g. passwords, must be appropriately managed so that the college can always access the information.
- Send data outside the UK without first obtaining written agreement from the Director of IT regard for the regulatory regime in the destination country.

Appropriate measures
To prevent any attempt to access Telford College's information from any external influences by either competitors and / or unauthorised personnel.

Approved Electronic File Transmission Methods
Includes supported File Transfer Protocol (FTP) clients and Web browsers.

Approved Electronic Mail
Includes all mail systems supported by the College's IT Infrastructure. These include, but may not be limited to, Microsoft Outlook mail client.

Approved Encrypted email and files
Zip-7 application files are encrypted to AES 256bit. Encryption software is available on staff personal computers.

Company Information System Resources
Includes, but not limited to, all computers, their data and programs, as well as all paper information and any information that is used for internal use.

Delivered Direct; Signature Required
Mail is left for pick up by postal service and or assigned carriers located at room E033, reception must be informed.

Envelopes Stamped Confidential
All Confidential document(s) are to be put into an envelope, which is sealed, addressed and marked "Confidential and for the addressee only". If sending the physical envelope of site via a third party, a reputable courier service must be used such as the Royal Mail Special Delivery Service.

Expunge
To reliably erase or expunge data on a PC or Mac, which is outside the machine's normal erasure routine, a separate program must be used to overwrite data – contact IT Helpdesk for advice.

Personal data
Information regarding living, identifiable individuals is to be treated as 'personal data'.

External network
This covers any use of mobile devices when processing College information. It is also provided by a third party (for example an ISP or mobile provider) or is part of the College's guest network provision.

Insecure Internet Links
All network links that originate from a local source or travel over lines that are not under the total control of Telford College.

Physical Security
Means having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable and access to systems is denied. For example, a laptop or other portable computer, it must never be left unattended

Private Link
An electronic communications path that Telford College has control over its entire distance of travel / transfer. For example, all Telford College networks are connected via a private link and using the RAS (Remote Access Software) to a connected employee's homes is a private link.

Encryption
Secure Sensitive Information in accordance with the *Acceptable Use Policy (AUP)*. Follow college guidelines on export controls on cryptography and consult IT Helpdesk and the Data Protection Officer for further guidance.

Data must be encrypted if it is:
- Stored on a computer or computer storage medium (CD, DVD, USB drive etc.)
- Transmitted via a computer network.
- Physically dispatched using a postal service
- It is being handled by the college and subject to an agreement with an **external organisation** specifying use of encryption, the agreed handling procedures, encryption technologies and standards must be used.

Physical security of information
Applies to all rooms which house confidential information whether in paper or electronic form:
- At all times, unattended offices must be kept locked including doors and windows,

- All confidential documents must be locked in secure means when not in use which includes using a minimum of two methods of security, for example, in a locked cabinet within a locked room.

Removal of confidential information from College sites
Is not to take place without the agreement and authorisation of the Data Protection Officer. A record must be kept (by the DPO and the removing department) of all information removed to include place date, type and index or all information moved away from a College site.

The college does not require staff or students to store or access confidential information using computing devices that the College does not own or manage.

Appendix 4 - The disclosure of student Safeguarding information.

Sensitive personal information, i.e. safeguarding information, is prohibited in references, if in doubt, then please contact the Data Protection Officer who will advise you on how to proceed. Please be aware that releasing this type of information without consulting the Data Protection Officer prior would result in a **severe data breach**.

There will also be instances of either the Local authority and or Police requesting information about a student, and in such circumstances, the request would have to be redirected to the Data Protection Officer and Safeguarding team.

Please note that Safeguarding information cannot be sent without prior approval from the Data Protection Officer before submitting any of the below-listed information.

- Physical violence
- Criminal behavior
- Inappropriate sexual behavior
- Peer on Peer Up skirting
- Substance misuse
- Disability/vulnerability
- Mental health
- Self-harm
- Legal highs
- Bullying others
- Arson
- Making undesirable contacts
- Medication

Student Reference Subject Access Request Process Flow diagram to third parties i.e. Employment Agencies, Screening Companies, Organisations and or any other institutions