Data Protection Policy 17/18

Created by	**MIS Director**	**June 2015**
Approved by	**Corporation**	**2015**
Version	**3.0**	
Updated by	**MIS Director**	**Feb 2018**
Date of next review		**June 2018**

DATA PROTECTION POLICY

1. Introduction

The Working Men's College is committed to providing wide access to education to all those who will benefit from it in an open and supportive environment for both learners and staff.

In order to deliver our mission we need to collect and use certain types of information about individuals and service users who come into contact with the College in order to carry out our work and secure funding. This personal information must be collected and dealt with appropriately whether it is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this.

There are changes to current legislation working their way through both the UK parliament and the EU. From 2018 – 2020 and possibly beyond, the legal landscape relating to data protection will change and the College aims to adhere to whichever legal requirements are in force at that time.

In recognition of this, it is expected that this policy document and related procedures will be reviewed every 6 months until an extended period of legislative stability is reached.

Data protection Act 1998 – in force until replaced by data protection bill currently going through parliament.

General data protection regulation (GPDR) – in force from 25th May 2018, covers all EU citizens.

New UK Data protection laws will be introduced sometime after Brexit is finalized, with GDPR still in force for EU Citizens after that date.

2. Data Controller and Data Processor

The Working Men's College is the Data Controller under the DP Act, which means that it determines what purposes personal information held, will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

The College is the Data Controller and Data Processor under GDPR.

3. Disclosure

The Working Men's College may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Individual/Service User will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law

allows College to disclose data (including sensitive data) without the data subject's consent.

These are:

a) Carrying out a legal duty or as authorised by the Secretary of State

b) Protecting vital interests of an Individual/Service User or other person

c) The Individual/Service User has already made the information public

d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights

e) Monitoring for equal opportunities purposes – i.e. race, disability or religion

f) Providing a confidential service where the Individual/Service User's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Individuals/Service Users to provide consent signatures.

The Working Men's College regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

The Working Men's College intends to ensure that personal information is treated lawfully and correctly.

To this end, The Working Men's College will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 1998.

Specifically, the Principles require that personal information:

a) Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met

b) Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,

c) Shall be adequate, relevant and not excessive in relation to those purpose(s)

d) Shall be accurate and, where necessary, kept up to date,

e) Shall not be kept for longer than is necessary

f) Shall be processed in accordance with the rights of data subjects under the Act

g) Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful

processing or accidental loss or destruction of, or damage to, personal information

h) Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Individuals/Service Users in relation to the processing of personal information

Or the principles as detailed in the GDPR from May 2018:

a) processed lawfully, fairly and in a transparent manner in relation to individuals

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

4. Data collection

The Working Men's College will ensure that there is a lawful basis for collecting and processing data. This will be from one of the reasons below but expected, in the most part, to be due to the data forming part of a contract, a legitimate interest or gathered by consent.

- Consent (positive opt in where GDPR applies)
- Contract

- Legal obligation
- Vital interests
- Public task
- Legitimate interests

The Working Men's College will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a paper based or online form.

When collecting data, the College will ensure that the Individual/Service User:

a) Clearly understands why the information is needed

b) Understands what it will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing

c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed

d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress

e) Has received sufficient information on why their data is needed and how it will be used

The College will endeavor to ensure that privacy notices and processing activities are referenced on relevant documentation with links to detailed information on the website.

Linked to this policy, the College will maintain separate and regularly reviewed policies covering:

- CCTV
- Acceptable use of ICT
- Records Management
- Information Security
- Freedom of Information

5. Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately. Appendix 1 details the overarching current document retention periods and should be reviewed annually.

The College will periodically contact former students / alumni to carry out surveys and case studies to comment on the positive impact their study has had on their lives. Any students not opted in will not be contacted.

It is the College's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

6. Data access, accuracy and security

All Individuals/Service Users have the right to access the information the College holds about them, unless an exemption applies.

The Working Men's College will also take reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition**,** The Working Men's College will ensure that:

- Our details are registered with the Information Commissioner with a named individual as a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Everyone processing personal information is appropriately trained to do so
- Everyone processing personal information is appropriately supervised
- Anybody wanting to make enquiries about handling personal information knows what to do
- It deals promptly and courteously with any enquiries about handling personal information
- It describes clearly how it handles personal information
- It will regularly review and audit the ways it hold, manage and use personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information
- Wherever practicable, access to personal information will be defined by the role being carried out, including the compartmentalisation of shared drives and role based access levels in relevant software packages
- All staff are made aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

7. Data breaches

The Working Men's College will notify the Information Commissioners Office (ICO) of any notifiable breaches within 72 hours of becoming aware of the breach. This includes instances where data has not been accessed but is 'locked' for over 24 hours in events such as ransomware attacks.

The College will also notify the data subjects in instances that represent a 'high risk' to the rights and freedoms of individuals.

The Working Men's College will ensure that:

- Staff understand what constitutes a breach
- A breach reporting procedure exists, with named individuals and defined responsibilities

8. General Approach

The Working Men's College will, through appropriate management and strict application of criteria and controls**:**

- Observe fully conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements
- Ensure the high quality of information used
- Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
    - The right to be informed that processing is being undertaken,
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information which is regarded as wrong information)
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred abroad without suitable safeguards

- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998, GDPR or other relevant legislation.

In case of any queries or questions in relation to this policy please contact the Working Men's College Data Protection Officer:

Name: Charlie Coles

Position: Management Information Services Director
(Data Protection Officer)

Date: 4th January 2018

Review Date: May 2018

DATA PROTECTION POLICY

Glossary of Terms

Data Controller – The person who (either alone or with others) decides what personal information the Working Men's College will hold and how it will be held or used.

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

General Data Protection Regulation (GDPR) – The EU legislation that provides a framework for responsible behaviour by those using personal information, coming into for in May 2018

Data Protection Bill – UK legislation working its way through parliament as a result of the incoming GDPR.

Data Protection Officer – The person(s) responsible for ensuring that the Working Men's College follows its data protection policy and complies with the Data Protection Act 1998.

Individual/Service User – The person whose personal information is being held or processed by the Working Men's College for example: a client, an employee, or supporter.

Notification – Notifying the Information Commissioner about the data processing activities of the Working Men's College, as certain activities may be exempt from notification.

The link below will take to the ICO website where a self assessment guide will help you to decide if you are exempt from notification:
https://ico.org.uk/for-organisations/guide-to-data-protection/exemptions/

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified, either directly or in conjunction with other information – e.g. name and address or learner number and ethnicity. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual learners, volunteers or employees within the Working Men's College.

Explicit consent – is a freely given, specific and informed agreement by an Individual/Service User in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data under DPA 1998.

Sensitive / special data – refers to data about:

- Racial or ethnic origin
- Political affiliations
- Religion or similar beliefs
- Trade union membership
- Physical or mental health
- Sexuality
- Criminal record or proceedings
- Genetics
- Biometrics

DATA PROTECTION POLICY

Appendix 1

Document retention guidelines
(for annual review by the named Data Protection Officer)

Wherever personal data underpins College income and is therefore auditable, the College will continue to retain the necessary documentation for defined time periods.

Government funded activity – 6 academic years from the year in which the activity ended.

European Social Fund (ESF) directly funded or match funded activity

- 2007 – 2013 ESF programme 31st December 2022
- 2014 – 2020 ESF Programme 31st December 2030

Other funded activity, including Charitable donations – Where the activity requires external financial audit, 6 academic years from the year in which the activity ended.

Any other activity not requiring external audit. 1 academic year from the end of the final year in which any activity took place.

Current year 2017/18 the standard 6 year document retention period ends August 2024.

In circumstances where specific defined conditions apply, documents will be kept for other defined periods.

A separate records management policy, covering document collection, retention and archiving holds more detailed information about time periods.