



DATA PROTECTION POLICY

Revision Status			
Rev No.	Details of Amendments	Name	Date
0	New Document	A. M. Information Services	
1	Update of College DPA statement New Reference to Appendix 4 – Staff Guidelines ESF document retention	A. M. Information Services	13/03/2008
2	Various references to Every Child Matters, Children’s Act 2004 and Education Act 2002	Requester: Director of Student Entitlement Added: A. M. Information Services	12/01/2009
3	Inclusion of Director of Student Entitlement and Information, Advice and Guidance as a Data Co-ordinator.	Requester: Vice Principal Quality & Standards Added: Assistant to V P Quality & Standards	14/01/2009
4	Update: 1. References to Learning And Skills Council with Skills Funding Agency and Young People’s Learning Agency 2. Reference to Learners, Staff, etc with Data Subjects	A. M. Information Services	12/04/2010

The responsibility for this policy rests with Director of Customer and Information Services acting as the Authorised Data Protection Officer for City of Wolverhampton College.

Contact Details:

**Director of Customer and Information Services, Paget Road Campus:
Internal Extension No. 7663**

Introduction

The Data Protection Act 1998 came into force on the 1st March 2000. It introduced a stricter regime of control over personal data and set out rules for processing personal information that apply equally to data recorded in automated systems, manual files and other storage media such as microfiche and CCTV.

The Act is a complex piece of legislation with a number of schedules, which lay down the criteria for the lawful processing of personal information.

Broadly speaking, the Data Protection Act 1998 works in two ways. It gives **data subjects (living individuals who are the subject of personal data)** certain rights. It also requires **data controllers (the legal entity processing the information)** to be open about how the information is used and to follow the eight principles of 'good information handling'.

The Act may be considered to empower the data subject and ensures transparency of processing by obliging data controllers to explain to individuals how their data will be used (Principle 1) and by providing the right of subject access under Section 7 whereby individuals can request access to their data. The importance of the right of subject access in Data Protection law cannot be underestimated: it is often only by exercising the right to see their information that individuals can determine whether other breaches of the legislation have occurred and to exercise their rights over the processing of that information.

Sharing information is lawful under the Duty of Confidence and Data Protection Act 1998. S11 Children's Act 2004 and S175 Education Act 2002 both recognise the statutory duty to share information to safeguard and promote the welfare of children. As part of Every Child Matters, 'Information Sharing: A Practitioners Guide' was issued in April 2006. This provides definitive guidance on sharing information legally and professionally and the College Data Protection Policy encompasses the 6 principles outlined in this guidance and the working practices of the College Child and Vulnerable Adult Protection Policy.

There are a number of exemptions available for defined processing purposes as well as criminal offences created by the Data Protection Act covering notification, processing and disclosure. The Information Commissioner has the right to serve an enforcement notice to cease processing upon any Data Controller who they are satisfied has or is contravening the eight principles. Thus control over this aspect of the College's arrangements is vital in ensuring statutory compliance and continuity of data processing.

There is a legal obligation imposed by the Data Protection Act to notify on the processing carried out and the College have a statutory responsibility to comply with the eight principles of the Act. Ensuring compliance with the principles is not simply an issue of operating within the law; it also requires procedures and controls to be in place for the effective handling of personal information and respecting the interests of data subjects.

City of Wolverhampton College's Statement of Intent towards the responsible compliance with the Data Protection Act 1998.

Privacy and Confidentiality

To operate an effective and efficient service, City of Wolverhampton College collects and processes information including personal information about the people that we deal with to allow us to, for example; organise courses, monitor performance, achievements and health and safety. These include current, past and prospective employees, learners, suppliers and others with whom we communicate. In addition, it may be a legal requirement to collect and use certain types of information, for example to comply with the requirements of the Skills Funding Agency, Young People Learning Agency and other Government Departments for business data.

We treat any information disclosed and entrusted to the College (e.g. by an employee, learner or applicant or by a third party), as strictly confidential and only process personal information as permitted by the Data Protection Act 1998.

Lawful Processing

To ensure the lawful processing of personal information, anyone processing personal data must comply with the eight enforceable principles of good practice, which state that personal data shall:

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

Sensitive Information

Information considered sensitive relating to data subjects, which is contained in paper form, and is to be transferred within the College will always be marked confidential.

Security Systems

We keep all information secure by using security systems and by training all authorised staff on their use. All file storage systems are kept locked at all times except when in use. Our security measures are reviewed on a regular basis and upgraded if necessary.

The technical control environment required to comply with the Seventh principle is additionally enforced through compliance with the College's IT Code of Conduct and Security Policy Guidelines.

Third Party requests for information

When third parties wish to get in touch with a data subject about whom we process data, we may pass on correspondence on their behalf, but we will never divulge the data subjects address or other details. Please see our internal processes for dealing with different types of requests, which is published separately as Appendix 4.

Information required by Police or Government Agencies

Requests for information about data subjects, received from the Police or Government Agencies such as the Inland Revenue or CSA are referred to Customer and Information Services to consider the nature of the enquiry and whether the information should be given. Exemptions within the Act will necessitate us to provide information which is reasonably required and requested in writing. eg safeguarding children.

Access to Personal Information held by us about Data Subjects

The Data Protection Act 1998 gives individuals the right to view personal information held about them.

We are committed to allowing individuals access to information that we hold about them which includes their own:

- Personal Files
- Learner achievements
- Processed applications/nominations/referral files
- Individual's (data subjects) can also request the deletion or amendment of incorrect information.

The following information cannot be made available:

- Information relating to or identifying a third party unless the person has given their written consent
- Information from other employers, colleges or agencies (eg. Social Services, Doctors, Lawyers) which could be reasonably expected to be treated as confidential
- Information that could cause physical or mental harm
- Information that could affect national security

We promise to be as open and helpful as possible and will provide a copy of specific information on payment of a small administrative charge, currently £10. We will respond to any request within 40 calendar days.

Management Control Infrastructure

To ensure the effective application of the Principles of the Act, management will:

- Nominate Data Co-ordinators within the organisation with the specific responsibility for data protection;
- Maintain an accurate and up to date Notification of processing purposes;
- Comply with the fair processing code regarding the collection and use of the data collected;
- Maintain the quality and accuracy of data held and processed;
- Periodically review the methods for handling and managing personal information collected and processed;
- Review the retention periods for which data is reasonably retained;
- Annually review all files and other documents to ensure information retained is up to date. Any obsolete information will be either deleted or shredded as appropriate and destroyed as confidential waste.
- Fully meet the rights of the data subject regarding data held and processed by the organisation;
- Take appropriate technical and organisational measures to protect personal data from unauthorised or unlawful processing and accidental loss, destruction or damage;
- Maintain the continuing education and awareness of staff processing personal data on behalf of the College to ensure that they understand their contractual and legal responsibility towards the personal information processed in their day to day work;
- Protect personal data from transfer outside of the EEA or where such transfer is necessary provide for adequate security of the information.

Status of the Policy

City of Wolverhampton College is required by the Act to notify the Information Commissioner of the use it makes of personal data and an entry has been made in the Data Protection Register. The College and all staff or others who process or use any personal information must ensure that they follow the principles of the Act at all times. In order to ensure that this happens, the College has developed this Data Protection Policy.

It is a condition for staff who deal with personal information at any time, to comply with the Data Protection Act 1998. Any member of staff who fails to follow the policy or who knowingly or recklessly uses, discloses or transfers personal information other than as prescribed in the College's notification may therefore be subject to disciplinary proceeding and could also be prosecuted.

Any member of staff, who considers that the policy had not been followed in respect of personal data about themselves or other data subjects, should raise the matter with the designated Data Co-ordinator initially. If the matter is not resolved it should be raised as a formal grievance. This in no way affects any statutory remedies available to that individual.

Notification of Data Held and Processed

All data subjects are entitled to

- Know what information the College holds and processes about them and why
- Know how to gain access to it. (Right to access information)
- Know how to keep it up to date
- Know what the College is doing to comply with its obligations under the 1998 Act

On request, the College will make available to all data subjects, a standard form of notification. This will state the types of data the College holds and process about them and the reasons for which it is processed.

Responsibilities of College Staff

The College will make guidelines and procedures available to staff, to ensure that the College is always working in compliance with the Data Protection Act 1998.

Human Resources will ensure that, all staff will have a regular opportunity to check that any information they have provided, to the College, in connection with their employment, is accurate and up to date. See Appendix 1

If and when, as part of their duties, staff collect information about other people (e.g. about learner's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff, which are at Appendix 2

Data Security

The College is responsible for ensuring that:

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

Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases. It may also result in prosecution by the Information Commissioner.

Personal data must be kept securely, ie:

- locked in a filing cabinet, drawer or room
- If it is computerised, be password protected;

Learner Obligations

Learners will be given the opportunity, at enrolment, to check that all personal data provided to the College is accurate. Learners on programmes of more than one year in duration will be asked to verify their details at the beginning of each academic year. Learners will have the statutory right to make a subject access request and view any information the College holds on them. As advised in the Learner Handbook, they will be asked that changes of address, etc are notified to the Customer and Information Services team or other member of staff as appropriate.

Learners who use the College's computer facilities will be expected to comply with the regulations and code of conduct set out in ICT Services ~ Acceptable Use Policy, as advised at induction and detailed in the Learner Handbook.

Right to Access Information

Data subjects within the business operations of the College have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the College's "Request for Learner Information" form (Appendix 3) which is available from Data Co-ordinators, Customer Services and Information Services. Please specify that this is a Data Subject Access Request. The College will supply copies of the information held. The College will make a charge of £10 on each occasion that full data subject access is requested.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days unless there is good reason for delay. In such cases, the reason for the delay will be explained in writing to the data subject making the request.

Staff requiring sight of their records should contact the Human Resource Manager.

Publication of College Information

Information that is already in the public domain is exempt from the 1998 Act. It is the College's policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

- Names and further details of College Governors
- Governor's Standing Orders and non-confidential papers
- The College's Annual Report
- The College Charter
- Summary of the College's Inspection Report

The College's internal phone list will not be a public document

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

Subject Consent

In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, **express consent** must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a learner onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

Some business operations (e.g. job roles, courses) will bring the applicants into contact with children up to the age of 18 and vulnerable adults. The College has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and learners for the courses offered. The College also has a duty of care to anyone interacting with the College and must therefore make sure that employees and those who use the College's facilities do not pose a threat or danger to other users.

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

By signing the College's Learning Agreement, learners are agreeing to the release of information as detailed in the following statement, which is contained on the reverse of the form. Any release of information that is not covered by this clause, must be requested in writing and be accompanied by the learner's permission. Please ask a Data Co-ordinator for a Request for Information Form.

“ Data Protection Act 1998 ~ You and Your Rights

During your time at the College, we will collect information about you. In order that you can progress through your course, it is important that this data is processed and stored securely within College for various purposes, which may include Enrolment Forms, ID Card Photographs, Registers, Achievements, References, Records of your College Work, Financial Records, Disciplinary Records. Please contact the College if you wish to know why this information is required. Information may be in both hard or electronic formats. Full records (paper and computer records) will be stored for the current and previous three academic years, after which time summary data (computer records only) will be held for a further three years, for statistical and reference purposes.

We may disclose certain information to your employer if sponsoring your studies, and your parents/guardians if you are under 19. Specific requests for information release to other third parties will be considered on the completion of the relevant form. We may disclose details of medical conditions you have told us (or a third party) about, where it is necessary for us to help safeguard your health and safety, or that of others. In the case of under 16 year olds, the College will normally liaise with your school, LEA and/or parents, as appropriate.

We have a statutory obligation to supply certain data to the Skills Funding Agency (SFA) and Young People’s Learning Agency (YPLA). Other organisations with which we may share information include relevant Awarding Bodies, the Department for Education and Skills, Connexions, Higher Education Statistics Agency, Higher Education Funding Council for England, educational institutions and organisations performing research and statistical work on behalf of the SFA/YPLA or its partners. The SFA/YPLA also administers the learner registration service (LRS) which will use your information to create and maintain a unique learner number (ULN). For further information about partner organisations and what they do, go to <http://www.SFA/YPLA.gov.uk> and follow the links to Data Protection.

Your course(s) may be part of a wider project which is co-financed by the European Social Fund (ESF). The SFA/YPLA is also a co-financing organisation and uses ESF from the European Union to directly or indirectly part-finance learning activities, helping develop employment by promoting employability, business spirit and equal opportunities and investing in human resources.

By signing the consent clause, you are agreeing to the processing of your personal and other data for any purposes connected with your studies or Health and Safety whilst on College premises, or for any other legitimate reason.

At no time will your personal information be passed to organisations for marketing or sales purposes.

Information will not be transferred outside The European Economic Area without subject consent. ”

Processing Sensitive Information

Sometimes it is necessary to process information about a data subject’s health, criminal convictions, race and gender and family details. This may be to ensure that College is a safe place for everyone, or to operate other College policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, data subjects will be asked to give express consent for the College to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the Data Protection Officer.

The Data Controller and the Designated Data Co-ordinators

The College as a body corporate is the Data Controller under the Act, and the board is therefore ultimately responsible for implementation. However, the Designated Data Co-ordinators will deal with day to day matters.

The College Data Protection Officer is available on Telephone Extension Number 7663.

In addition, the College's designated Data Co-ordinators include:

The Senior Management Team, Faculty Directors, Faculty Co-ordinators, Assistant Managers for Customer and Information Services and Director of Student Entitlement and Information, Advice and Guidance.

Full details of who to contact are held by the Data Protection Officer or on the College Intranet – Staff Directory – Data Co-ordinators

Examination Marks

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

Retention of Data

The College will keep some forms of information for longer than others. In line with the Data Protection Act's 5th Principle of Good Practice and storage requirements, information about data subjects cannot be kept indefinitely. In general, data subject's computerised records will be kept for a maximum of seven years after they leave the College. This will include any personal information provided to the College.

For learners, all other information, including any information about attendance, learning support, health or disciplinary matters will be destroyed within 3 years of the course ending and the learner leaving the College.

The exception to this would be if the learner's course is sponsored by European Social Funds. Full records will be retained for the life of the ESF project and then for a further seven years.

For staff, the College will need to keep information for longer periods of time. In general, all information will be kept for a minimum of seven years after a member of staff leaves the College. 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 their employment, and information required for job references. A full list of information with retention times is available from a Data Co-ordinator.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the College. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the College's Data Protection Officer.

HUMAN RESOURCES

PERSONAL PROFILE

Date

Please check the details below for errors and/or omissions. Should an error and/or omission have occurred please correct writing clearly in red ink. Only return this form to Human Resources if the information is incorrect.

PERSONAL DETAILS

Name:

Tel No:

Address:

NI No:

Gender:

Disability:

Post Code:

Ethnicity:

EMERGENCY CONTACT DETAILS

CONTRACT DETAILS

Contract Type:

Pay No:

Continuous Service Date:

Temporary:

Grade Name:

Hours Per Week:

Job Title:

Faculty/Department:

School/Section:

QUALIFICATIONS

Qualification

Qualification Grade

APPENDIX 2

Data Protection Policy - Staff Guidelines

Purpose

City of Wolverhampton College processes information about its data subjects e.g. Employees, applicants, learners, past and present, or other individuals for purposes such as the administration of the admissions process, the effective provision of academic and welfare services and to operate the payroll. This policy aims to ensure that in so doing the College complies with the Data Protection Act 1998 ("the Act") and that personal information is collected and used fairly, stored safely and not disclosed to any third party without express permission from the individual.

Scope

This policy applies to all staff where they are acting in the course of their duties as its employees, and to learners and other members of the College where they are acting on its behalf or under its instruction.

It applies to all personal data processed in the course of the activities described above, regardless of format (paper, digital or audio-visual) and location (processed on College premises or elsewhere). Personal data are any data relating to an identified individual or to an individual who may be identifiable from those data if put together with other data.

Responsibilities under the Act

Data Protection Principles

The College, as a Data Controller, must comply with the Data Protection Principles, which are set out in the Act. In summary these state that personal data shall:

- Be processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for specified and lawful purposes and shall not be processed in any manner incompatible with those purposes.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for those purposes.
- Be processed in accordance with the data subject's rights under the 1998 Act.
- Be the subject of appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country or territory has equivalent levels of protection for personal data.

Processing

Staff Checklist for Processing Data

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

- do you really need to collect the information?
- do you really need to collect all of it?
- is the information 'ordinary' or is it 'sensitive'?
- do we have the data subject's consent? Is it unambiguous and freely given?
- are you authorised to collect/store/process the data?
- unless the data have been obtained from a reliable source, have you checked with the data subject that the data is accurate?
- are you sure that the data are secure?
- if you do not have the data subject's consent to process, are you satisfied that you do not need it?
- for how long should the data be retained? When should it be updated or destroyed?
- What steps should be taken to ensure that this happens?
- Who are you sending the data to? Is this authorised?

“Processing”, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data,
- retrieval, consultation or use of the information or data,
- disclosure of the information or data by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data.

Data Sharing

Key principles to inform the decision to share:

- Is the information confidential?
- Consent required to share?
- Statutory duty to share
- Share the right information correctly
- Record the decision

“The Data Protection Act is not a barrier to sharing information but it is in place to ensure that personal information is shared appropriately” Information Commissioner.
www.ecm.gov.uk/informationsharing

Data Controller

The College is the Data Controller.

Notification to the Information Commissioner

The College has an obligation as a Data Controller to notify the Information Commissioner of the purposes for which it processes personal data. Individual data subjects can obtain full details of the College’s data protection notification with the Information Commissioner from the College Data Protection Officer or from the Information Commissioner’s website (www.ico.gov.uk).

Data Protection Officer

The College Data Protection Officer is the Customer and Information Services Director. All queries about the College policy or ‘out of the ordinary’ requests for access to personal data should be addressed to the Data Protection Officer.

Data Co-ordinators

The College will designate staff in each area as “Data Co-ordinator”. These will include the Senior Management Team, Faculty Directors, Faculty Co-ordinators and Assistant Managers for Customer and Information Services. Full details are available from the Data Protection Officer. The Data Co-ordinators will be the only staff who can release information to authorised third parties that is sensitive or not standard data.

Data Processors

All members of the College who process personal data in any form must ensure they comply with the requirements of the Act and with the College’s data protection policy (including any additional data protection procedures and guidelines that may be issued by the College from time to time).

In particular, no member of the College may, without the prior written authorisation of the Data Protection Officer:

- develop a new computer system for processing personal data;
- use an existing computer system to process personal data for a new purpose;
- create a new paper filing system containing personal data;
- use an existing paper filing system containing personal data for a new purpose.

The above does not apply to databases which are maintained by individual College employees for their private domestic uses, for example, private address books. However, individuals should consider whether their private domestic uses fall within the scope of the Act. A breach of the Act and/or the College’s data protection policy may result in disciplinary proceedings.

Staff Checklist for Data Creation

The Act means that any recorded opinion about or intentions regarding a person are personal data to which a data subject may gain access. This should be borne in mind when written or other records are made (and this includes hand written notes, e-mails and audio recordings, in addition to computer and manual files) and when information is to be destroyed. The following is a useful test to apply to 'doubtful' comments

- Is this comment fair, accurate and justifiable?
- If I were to show this to the data subject, would I still be confident that the comment is fair, accurate and justifiable?

If the answer to the questions - and in particular the first question - is 'No', then the comment should go unrecorded

Data Security and Disclosure

All members of the College are responsible for ensuring that:

- Any personal data they hold is classified and managed in accordance with the College's Information Security Policy.
- Personal data is not disclosed to any unauthorised third party, and that every reasonable effort will be made to see that data is not disclosed accidentally. Unauthorised disclosure is a disciplinary matter and may be considered gross misconduct. If in any doubt, consult the College Data Protection Officer.
- Personal data must be kept securely and examples of how this may be done include:
 - keeping the data locked in a filing cabinet, drawer or room,
 - if the data is computerised, ensuring that the data is password protected.

Request for Learner Information

To be signed by the learner for whom the information has been requested.
 An individual's permission is required to pass on information, to any third party, not described on their College Learning Agreement. All information given to City of Wolverhampton College is held and processed under the Data Protection Act 1998.

An administration fee of £10 will be charged for a full copy of the learner's College records.

Learner ID	<input style="width: 100%;" type="text"/>		
Surname	<input style="width: 100%;" type="text"/>		
Forename(s)	<input style="width: 100%;" type="text"/>		
Main Course	<input style="width: 60%;" type="text"/>	Year	<input style="width: 20%;" type="text"/> / <input style="width: 20%;" type="text"/>

<p><i>If different from</i> INFORMATION REQUESTED BY/FOR Company Name Address</p> <p>Telephone Number</p>	
<p>Format Required <i>Tick as appropriate</i></p>	<p>VERBAL CONFIRMATION <input type="checkbox"/></p> <p>LETTER <input type="checkbox"/></p> <p>FAX <input type="checkbox"/></p>
<p>Detail Required <i>Tick as appropriate</i></p>	<p>START / END DATES <input type="checkbox"/></p> <p>GUIDED LEARNING HOURS <input type="checkbox"/></p> <p>HOURS PER WEEK <input type="checkbox"/></p> <p>FULL~TIME / PART~TIME <input type="checkbox"/></p> <p>EXAMINATION RESULTS <input type="checkbox"/></p>
<p>Further Information Required</p> <p>Date required by: <input style="width: 100%;" type="text"/></p>	

I give my permission for City of Wolverhampton College to release information, as detailed above :

Learner Signature <input style="width: 90%;" type="text"/>	Date <input style="width: 90%;" type="text"/>
---	--

College Use Only : COMPLETED <input style="width: 90%;" type="text"/>	Date <input style="width: 90%;" type="text"/>
--	--