YMCA
GEORGE WILLIAMS
COLLEGE

DATA PROTECTION POLICY AND PROCEDURES

MAY 2018

Date Policy Last Approved	Approved	Review Frequency	Date of next Review
May 2018	Finance & Audit Committee	Annually	May 2019

INDEX

Introduction

1. In order to carry out its role as a provider of training and education George Williams College ("GWC") is required to retain certain information about its staff, students and other users. This information is used to monitor performance, achievements and ensure the safety of its staff and students. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and the Government complied with. In line with article 5 of the General Data Protection Regulation, GWC will comply with the following data protection principles and will ensure that personal information is:

 Processed in a lawful, fair and transparent manner

 Collected for a specified and legitimate purpose – and not processed in a manner which is incompatible with those purposes

 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

 Accurate and, where necessary, kept up to date;

 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;

 Processed in a manner that ensures appropriate security of the personal data

2. GWC staff and others who process or use any personal information must ensure that they follow these principles at all times. This Data Protection Policy and Procedures document is intended to ensure that this happens.

Status of the Policy

3. This policy does not form part of the formal contract of employment for staff but it is a condition of employment that employees will abide by GWC rules and policies.
4. Any failure to follow the policy can, therefore, result in disciplinary proceedings. Any member of staff who considers that the policy has not been followed in respect of personal data about a student or themselves should raise the matter with the designated controller within their area of work within the College, in the first instance. If the matter is not resolved, it should be raised as a formal grievance under the College's Grievance Procedures.

Designated Data Controllers and the Data Protection Officer

5. As a public authority as defined by data protection legislation the College is required to comply with the General Data Protection Regulation (GDPR). Whilst ultimate responsibility for compliance rests with the GWC Board, the day to day compliance to GDPR is the responsibility of all members of staff and the management of the College.
6. In order to ensure ongoing compliance with data protection legislation there is a steering committee which meets once a term to oversee the management and control of data. This steering college is chaired by the Director of Governance who also serves as the College's Data Protection Officer. The remaining members of this committee consist of designated data controllers for key areas of the College's operations. The grid below gives details of these data controllers:

Department within the College	Designated Controllers
GWC FE/HE teachers / lecturers	College CEO
Registry / Examinations	College CEO
Finance	CFO
Business Development	Head of Business Development
Human Resources	Head of Human Resources

7. Under the GDPR legislation it is mandatory to appoint a data protection officer. This role is performed by the CEO whose key responsibilities are to:
 Inform and advise the data controllers and processors with regards to data protection legislation
 Monitor compliance with data protection legislation
 Provide advice with respect to data protection issues
 Co-operate with the Information Commissioner's Office (ICO)
 Act as a point of contact
 Chair the college's data protection steering college

Rights of Students and Staff

8. All staff and students and other users for whom the college may hold personal information (data subjects) are entitled to the following rights:
 the right to be informed
 the right of access
 the right to rectification
 the right to erasure
 the right to restrict processing
 the right to data portability
 the right to object
 rights in relation to automated decision making and profiling.

9. The College provides all staff and students and other relevant users with a standard form of notification. This will state all the types of data the College holds and processes about them and the reasons for which it is processed.

Responsibilities of Staff

10. All staff are responsible for:
 checking that any information that they provide to the College in connection with their employment is accurate and up to date;
 informing the College of any changes to information which they have provided e.g. change of address;
 checking the accuracy of information that the College will send out from time to time giving details of information kept and processed about staff;
 informing the College of any errors or changes (the College cannot be held responsible for any errors unless the staff member has informed the College of them)

11. If and when, as part of their responsibilities, staff collect information about other people (i.e. about students' course, work, opinions about ability, references to other academic institutions or details of personal circumstances) they must comply with the guidelines for staff which are included as Appendix 1.
12. Staff should not pass personal information or work contact details of colleagues if a request is made from an external source, unless permission has been received from the staff member in question. In normal circumstances, if a request is made for contact details then the external person should be asked to make a request in writing (usually via email) which provides their contact details and allows the staff member in question to contact them if they deem this to be appropriate.
13. Staff must note that it is a criminal offence to use personal data that they have access to as part of their work and use it for their own personal or commercial reasons, and can lead to prosecution.

Data Security

14. All staff are responsible for ensuring that any personal data which they hold is kept securely (personal data is defined as any information relating to an identified or identifiable natural (living) person. With respect to most personal information the College has a legitimate reason for holding and processing personal data because it needs to do in order to carry out its obligations with respect to a funding contract or there is a legal obligation to do so.
15. Some personal information processed by the College will be sensitive. In most instances, the College will require consent from staff or students to hold this information, however in some cases the College may hold or process sensitive information for legitimate reasons. Sensitive personal data is defined as information with respect to the following:
 racial or ethnic background
 political opinions
 religious or other beliefs
 trade union membership
 physical or mental health conditions
 sexual orientation
 criminal offences, criminal proceedings and convictions
 genetic and biometric data

16. Personal information will not be disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party. This includes visual images held as part of the College's ID card system and the CCTV security system. Personal information should be:
 kept in a locked filing cabinet or in a locked drawer or, if it is computerised, - be password protected or
 kept only on a disk/USB which is itself kept securely or kept in a locked office with restricted access

17. CCTV images must be kept securely and be password protected – the appropriate documentation must be provided by Police and other Government Agencies quoting the DPA section. Internal request must be sanctioned by the Data Controller for the Centre using the CCTV Subject Access Request form in Appendix 4. Please also find an overview of the College's CCTV Policy.
18. Staff should note: 6

 that unauthorised disclosure will normally be considered as a disciplinary matter
 read this policy in conjunction with the College's ICT Acceptable Use policy.

Student Obligations

19. Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that all changes of address etc are notified to their personal tutor, who should notify the registry team. Students who use the College's computer facilities may from time to time have access to personal data about themselves. The College can bear no responsibility for the sharing of personal information if this is carried out by the student themselves.

Conditions for Using Personal Data

20. The processing and holding of personal information can only be carried out if there is legitimate reason for doing so. In order to carry its primary powers as an FE institution (i.e. to provide education and training) the College is permitted to hold personal information about staff and students, such as their name, contact details and academic achievement to date. If there are legitimate reasons for holding information then the College is permitted to do so. These reasons (conditions for using personal data) are as follows:

1. Consent
2. Performance of a contract
3. Legal obligation
4. Vital interests
5. Public interest or exercise of official authority
6. Legitimate interests

Consent and Processing Sensitive Information

21 In some instances where personal sensitive information is processed the College will require staff or students to provide consent. The College adheres to the definition of consent as defined within the GDPR legislation which is as follows:

Consent is 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.."

22. It is therefore the policy of the College that where personal sensitive information is held and does not fit within the definitions provided for the conditions for using personal data which are not legal or contractual (i.e. reasons 2-6 from above) then consent will be sought in an unambiguous manner.

23. In order to ensure a safe work place and that the College complies other areas of the law, such as equal opportunities there is a requirement to process sensitive information in relation to gender, race, criminal convictions or health. Also in some instances, the processing of some types of personal data is a condition of acceptance of a student onto a course and is a condition of employment for staff. Because this information is considered sensitive, it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give 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 designated data controller. 7

24. The College may also ask for information about particular health needs such as allergies to particular forms of medication or foods or any conditions such as asthma and diabetes. The College will only use the information in the protection of the health and safety of the individual and in the event of a medical emergency. Therefore, all prospective staff and students will be asked to sign a consent form regarding particular types of information when an offer of employment or a course place is made
25. Some jobs or courses will bring staff and applicants for posts at the College and some students into contact with children including young people between the ages of 16 and 18 years. The College has a duty under the Children Act and other legislation to ensure that they are suitable for the job and students for the courses offered. The College also has a duty of care to all staff and students and must therefore ensure that employees and those who use the College's facilities do not pose a threat or danger to other users

Data Sharing

26. GWC will comply with the relevant legislation with respect to the sharing of personal information. For example, if the Police make a request for personal information associated with carrying a criminal investigation the College will share personal information as long as a legitimate reason is provided and the appropriate form complete. Also GWC is also required to supply personal information if requested to the relevant local child protection / safeguarding Board in line with its duty of care to those students who under the age of 18 or are classified as a vulnerable adult. In all cases the designated controller for the relevant area of the College must agree to the request and authorisation must be sought be the member of staff who is sharing the information.
27. When sharing personal information in line with approved and authorised protocols (for example if a query is being made by or with a funding agency) then personal information must be sent in encrypted format.

Rights to Access Information

28. Students, staff and other data subjects of the College have the right to access any personal data that is being kept about them either electronically or in manual filing systems. Any person who wishes to exercise this right should complete the Access to Information form and give it to their personal tutor or relevant manager or head of their section, department or service area (see Appendix 2)
29. The College aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 21 working days unless there is a good reason for delay. In such cases, the reason for delay will be explained, in writing, to the data subject making the request.

Examination Marks

30. Students are entitled to information about their examination marks for both course work and examinations. Students are to be made aware that they are not entitled to view this information prior to the official publication date. The publication of examination results at an individual level requires the consent of the individual concerned. The College however may use data on an anonymous and combined basis to carry out analysis of performance in relation to teaching, 8

learning and assessment

Retention of Data

31. The College will keep some forms of information for longer periods of time than others. Constraints on storage space determine that information about students cannot be kept indefinitely unless there are specific requests to do so. In general, information about students held in manual files will be kept for a maximum of five years after the student has left the College. This will include:

- name and address
- academic achievements including marks for course work
- copies of any references given

32. A retention of records schedule is attached.

Conclusion

33. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken or access to GWC facilities being withdrawn and even a criminal prosecution (if there is evidence that personal information has been used for personal gain). Any questions or concerns about the interpretation or operation of this Policy should be taken up with the designated relevant data controller or the Data Protection Officer.

APPENDIX 1

STAFF GUIDELINES FOR DATA PROTECTION

1. All staff will process data about students on a regular basis when marking registers, writing reports or references or as part of a pastoral or academic supervisory role. The College will ensure, through registration procedures, that all students give their consent to data processing and are notified of the categories of processing. The information staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:

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

2 Information about a student's physical or mental health, ethnicity or race, is sensitive and can only be collected and processed with the students' express consent. If staff need to record this information, they should use the standard form e.g. Student Services may want to keep information about dietary needs for religious or health reasons prior to taking students on a field trip, or that a student is pregnant.

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

 up to date
 fair
 kept and disposed of safely and in accordance with the College policy

4. Staff must not disclose personal data to any student unless for normal or academic or pastoral purposes without authorisation or agreement from the designated Data Controller or in line with the College policy.

5. Staff shall not disclose personal data, about staff or students, to any other staff member except with the authorisation or agreement of the designated Data Controller or line with the College policy.

6. Staff should understand their responsibilities for data protection and security when dealing with personal data on computers or in files away from the workplace or by means of log- ins to the College network from home or away from the work environment:

 if the computer, laptop, tablet or mobile belongs to the College then it is not used by other household members
 only equipment designed to be portable is taken from the workplace
 if it is their own computer then College data is not accessible to anyone else i.e. password protected and all files are deleted when no longer needed
 virus protection is in place
 any print-outs are stored and disposed of carefully
 suitable transport is provided between home and work so that equipment data and manual files remain secure whilst in transit.
 any loss, unauthorised destruction, or disclosure of data may result in disciplinary investigation.
 computer files brought to work from outside the College environment are virus checked before loading onto the Colleges' computer equipment
 no personal files, containing information about staff or students, can be taken from the College environment without the express permission of the Line Manager and/or the Data Protection Policy

designated Data Controller. Staff will be asked by their Line Manager/designed Data Controller to complete an authorisation form, which should be signed and dated by their Line Manager and/or the designated Data Controller. Personal data files must not be left unattended at any time except when locked in a filing cabinet drawer or similar equipment
 Staff should not hold personal data belonging to students on their mobile phone, unless they have gained express permission from the student/s in question.

7. Before processing any personal data, all staff should consider:
a) whether the information needs to be held by GWC and does the holding of information fit within the purposes of providing education and training;
b) if there is additional information that we are asking the student to supply e.g. ethnicity, has the student / staff member given express permission for GWC to process and store this information.

8. Staff should never share personal information without being sure that they are permitted to do so. If in doubt staff should check with their data controller who in normal circumstances will be the Director of their service area.

APPENDIX 2

STANDARD REQUEST FORM FOR ACCESS TO PERSONAL DATA (STUDENTS)

I **[insert name]** …….. wish to have access to either **(delete as appropriate):**

1 All the data that the College currently has about me either as part of an automated system or part of the relevant filing system, or

2 Data that the College has about me in the following categories:

- **Academic marks or course work details**
- **Academic or employment references**
- **Disciplinary records**
- **Health and medical matters**
- **Any statement of opinion about my abilities or performance**
- **Personal details including name, address, date of birth etc**
- **Other information (Please specify)**

Name (in full)
Student number: :
College course attended
Date of Birth
Address to which information is to be sent:
Daytime contact telephone number:
For Office Use Only
Request for information received on ……..
Information sent to enquirer on ……..
Signed (Designated Date Controller ……

APPENDIX 3

DATA PROTECTION AGREEMENT

1 **Data Protection**
i) All staff are required to abide by the College Data Protection Policy, a copy of which is included as part of the induction information.
ii) A failure to follow any of the guidelines in relation to collection, keeping, processing or destruction of any personal data whether regarding another staff member, student or other third party and whether deliberate or accidental will be regarded as potential misconduct and may result in disciplinary proceedings being brought.
iii) Deliberate or negligent misuse of data whether by unlawful disclosure or otherwise may be considered gross misconduct and may result in the summary dismissal in the most serious cases

2 **Consent to process**
The employee agrees by virtue of this contract to George WIlliams College processing such information as may be necessary for the proper administration of the employment relationship both during and after employment provided that proper regard is had to such data protection principles as may be in force. In particular, the employee consents to the following information being processed for the purposes set out below. Any information about:
 Mental and physical health including dates of absence from work due to illness and the reasons for the absence
 Matters relating to pregnancy and maternity leave
 Criminal convictions
 Race or ethnic origin
 Professional qualifications
 Matters of discipline
 Pensionable pay or contributions
 Age and years of service
 Membership of recognised trade unions

3 This information may be processed for any of the following reasons:
 Payment of salary, pension, sickness benefit or other payments due under the Contract of Employment
 Monitoring absence or sickness under an absence controlled or capability policy
 Training and development purposes
 Management Planning
 Negotiations with the Trade Union or staff representatives
 Redundancy and succession planning
 Curriculum planning and organisation
 Timetable and organisation
 Compliance with equal opportunities policy
 Compliance with the Disability Discrimination Act
 Carrying out checks with respect to child protection registers Data Protection Policy

APPENDIX 3 (cont)

Occupational sick pay

4 In order to administer the occupational sick pay and leave scheme, all staff are required to provide information about their absences and the reasons for it. In some cases, this will be by way of self-certification. Non provision of this information could result in delays or non-payment of sick pay.

Recruitment literature GDPR

B The College collects and keeps information from job applicants so that we can send details of future job opportunities to you. We keep your name and address and details of your application. If you do not want us to do this, please indicate by ticking the box below.

I do not want you to keep my details on file if I am unsuccessful in my application [Y]/ [N]

Tick as appropriate