Humber UTC
A University Technical College

Data Handling Policy

July 2017

Marc Doyle

Approved by the Humber UTC Governing Body on XXXX

Document control table

Document title:	Data Handling Policy
Author (name & job title):	Marc Doyle, Principal & CEO Kathryn Bower, HR Consultant
Acknowledgement	Adopted from Outwood Grange Academies College
Version number:	V1 July 2017
Date approved:	XXXXXX
Approved by:	HUTC Board
Date of review:	July 2018

Document History

Version	Date	Author	Note of revisions

1. Introduction

Humber UTC needs to collect and use data concerning its staff, students and other individuals who come into contact with it for a variety of purposes including the recruitment and payment of staff; the organisation and administration of courses; the monitoring of health and safety arrangements; the monitoring of performance, achievements; and compliance with statutory obligations, government agencies and other bodies.

In collecting and using data, the college must comply with the requirements of the Data Protection Act 1998 and the Data Retention Regulations 2009 that govern the processing and retention of personal data. Under these requirements, the information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully, and the Data Protection Principles must be followed. In summary, these principles state that personal data shall:

- Be processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained only 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 Act.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The college and all its staff, students, or others who process or use any personal information must ensure that they follow these principles at all times. This policy seeks to ensure that this happens.

2. Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the college from time to time. Any failure to follow the policy can therefore result in disciplinary proceedings.

Any student or member of staff who considers that the policy has not been followed in respect of any personal data concerning them should raise the matter with the college's Data Director.

3. College as Data Controller

The college is the data controller under the Act, and is therefore ultimately responsible for its implementation. However, the college's Data Director will deal with day-to-day matters.

In accordance with the requirements of the Act, the college is registered as a data controller with the Office of the Information Commissioner.

The college stores data in secure conditions and will only process or disclose data within the terms of its notification to the Information Commissioner. Details are given in an Appendix of the **purposes** for which the college processes data and of the bodies to whom it **discloses** information. These indicate the nature of the college's notification, but are not exhaustive.

Any member of staff or student wishing to make specific enquiries about their data should in the first instance contact the college's Principal.

4. Rights of Data Subjects

4.1 Notification to Staff, Students and other Data Subjects

All staff, students/parents and other data subjects 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 1998 Act.

The college will ensure, through this policy and the issue of further guidance as necessary, that staff, students/parents and other data subjects are notified of the above as appropriate.

4.2 Right of Access to Information:

The 1998 Act gives all individuals whose personal information is stored by the college ("data subjects") the right to access any information that relates to them, whether it is held on a computer system or in a manual filing system.

The 1998 Act also sets out specific rights of access for college students to their educational records held by their college. Educational records are the official records for which head teachers are responsible. Parents also have their own independent right of access to their children's educational records under the Education (Pupil Information) (England) Act 2000. Because parents have this independent right of access to student records a student has no right to prevent their parents from obtaining a copy of their college records.

The college aims to comply with requests for access to personal information as quickly as possible and will ensure that requests for access are dealt with within the timescale specified by legislation. Request for access made by students and parents must be dealt with within 15 college days and requests made by all other data subjects should be dealt with within 40 days. If, for any reason, these timescales cannot be met, the reason will be explained in writing to the data subject making the request.

Any person wishing to exercise their right of access should put the request in writing to the college Principal.

4.3 Right to object to Data Processing:

Staff, students and other data subjects have a right to object to data processing that causes them damage or distress. Any member of staff, student or other data subject who wishes to register an objection must do so in writing, by letter addressed to the college.

5. Accuracy of Data

All staff are responsible for:

- Checking that any information 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 information that the college may send out from time to time giving details of information kept and processed about staff.

Students/parents must ensure that all personal data provided to the college is accurate and up-to-date. They must notify the college of any alterations to their address or personal details as provided on their timetable sheet.

The college cannot be held responsible for any errors unless the member of staff or student/parent has informed the college about them.

6. Staff/Student Processing of Data

If and when, as part of their responsibilities, staff collect information about other people (e.g. about students' work and grades, opinions about ability, references from external bodies, or details of personal circumstances), they must comply with the guidelines for staff. In particular, staff must ensure that any personal data which they hold is kept secure and that personal information is not disclosed either orally, in writing, or accidentally or to any unauthorised third party.

7. Sensitive Data

Sensitive data covers the following types of information:

- Disability
- Racial origins
- Political opinions
- Trade union membership
- Sexual life
- Religious beliefs or beliefs of a similar nature
- Court proceeding, criminal convictions or allegations
- Physical health records

Sensitive data will only be processed under strict conditions, which include:

- Having the explicit consent of the individual.
- Being required by the law to process the data for employment purposes.
- The information is needed in order to protect the vital interests of the data subject or another.
- Dealing with the administration of justice or legal proceedings.

8. Retention of Data

Information about staff and students will be kept in line with the Data Retention Regulations 2009, the college's Data Retention Policy and statutory requirements.

9. Compliance

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 the college's facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should in the first instance be taken up with the Principal.

APPENDIX 1 - DATA TYPES & USES

1 Purposes

The College collects and uses data about its staff and students for the following purposes:

Staff

- Organisation and management of the college.
- Payment of salaries, wages & pensions.
- Vetting.
- Disciplinary matters.
- Membership of a Trade Union and/or of professional body or society to facilitate payment of subscriptions.
- Medical history to ensure suitability for appointment.
- CCTV monitoring of college site.
- Seeking improvements in health and safety.
- Staff development.
- Recording of ethnic origin and disability. This information is requested on a voluntary basis and is used to enable the college to evaluate the operation of its equal opportunities policy.
- Recording of periods of sickness to enable payment of statutory sick pay.
- Providing employment references.

Students

- Central and departmental administration (includes personal and academic details) and management of academic processes (e.g. CATs, SATs, progress grades, external & internal exam results).
- Provision of advice and support to students (through the Pastoral System, the Counselling Service, Work Experience and the Careers Service).
- Student ID cards.
- Library cards.
- Planning & administration of trips & events.
- Seeking improvements in health and safety.
- CCTV monitoring of college site.
- Monitoring & recording of ethnic origin and disability. This information is requested on a voluntary basis and is used to enable the college to evaluate the operation of its equal opportunities policy.

2 Disclosure of Information

The college discloses information about its staff and students to the following:

Staff

- Data subjects themselves.
- Guardians of the data subject.
- Current, past or present employers of our staff.
- Healthcare, social and welfare practitioners.
- Potential providers of education to our staff.
- External agents employed by the college in the conduct of its business.
- Police forces.
- Local and central government.

Students

- Data subjects themselves.
- Parents, guardians or other persons with parental responsibility.
- Current or potential employers of our students.
- Current or potential providers of education to our students.
- External agents employed by the College in the conduct of its business.
- Healthcare, social and welfare practitioners.
- Local government.
- DfE.
- Careers service.
- The media.
- Voluntary & charity organisations.

3 Restrictions on Disclosure

Disclosures to persons or institutions not listed above will be made only with the permission of the member of staff or student unless exceptional circumstances apply, as provided by law.

APPENDIX 2 - GUIDELINES FOR STAFF - GENERAL

1 Introduction

The college has adopted a Data Protection Policy covering the arrangements made by the college to implement the requirements of the Act. All staff must be aware of and ensure that they comply with the Policy. The following guidelines are intended to assist staff to understand the aim of the Act and what is meant by personal data and to set out the main areas in which staff are likely to be affected by data protection issues in the course of their work. The guidelines do not attempt to cover every situation. Further information and advice is available from any member of the Leadership team.

2 Aim of the Act

The main aim of the Act is not to protect data itself, but to provide an individual with some control over the use of their personal data, in particular unforeseen secondary uses, and to provide protection from unwanted or harmful uses of the data. The intention is not, therefore to cut off the flow of data, but to see that it is collected and used in a responsible way. To achieve this aim, the college, as a data controller, needs to have in mind the following key concepts:

- Purpose – The college should process personal data only when it has a clear purpose for doing so.
- Fairness – There are many legitimate purposes for processing personal data, even where individuals may not wish this to happen. For processing to be fair, the individual must be informed of the purposes for which her/his data is to be processed. Processing will also only be fair when it meets one of a number of criteria set out in the Act, for example, that it is necessary in order to pursue the legitimate interests of the college.
- Transparency –Individuals have the responsibility for enforcing their rights, so to enable them to do so, they need to know the purpose of the processing and the measures the college has taken to ensure that the processing is fair.

3 Personal Data

Personal data means any data relating to a living individual who can be identified from the data (including photographs and videos), or from the data and other information that the college has in its possession, or which is likely to come into its possession. Personal data also includes any expression of opinion about the individual and any indication of the college's intentions, or any other person, in respect of the individual. The data includes information that is:

- Being processed by computer.
- Recorded with the intention that it should be processed by means of computing equipment.
- Recorded manually as part of a filing system or with the intention that it should form part of a filing system.

It should be noted that personal data processed via World Wide Web tools and other Internet software are included in the above.

4 Staff Processing of Data

Staff processing data as a legitimate part of their employment (e.g. teaching, administration), do so under the college's notification to the Information Commissioner. The main areas covered in the notification are listed in the college's Data Protection Policy.

Many staff process data about students on a regular basis. Much of this will be non-sensitive data, but some may be sensitive and will require explicit consent from the student. Examples are given under the headings below.

Students/Parents are informed of the purposes of processing through college prospectuses & student handbooks.

Staff wishing to use personal data for research purposes need to ensure that they comply with the Data Protection Principles (although there are exemptions from some of the principles in some circumstances). As clear guidance as possible should be provided to individuals whose personal data is to be used in the research as to why the data is being collected and the purposes for which it will be used.

Staff responsible for processing data should ensure that they use the checklist at the end of this section.

Non-sensitive Data

The information that staff deal with on a day-to-day basis will be 'non sensitive' and will cover categories such as:

- General personal details, such as, for example, name and address.
- Details about class attendance, marks and grades and associated comments.
- Reports and references.
- Notes of personal supervision, including matters about behaviour and discipline.

Sensitive Data

Information about a student's physical or mental health, sexual life, political or religious views, Trade Union membership or ethnicity or race is sensitive and can only be collected and processed with the student's express consent. If staff need to record this information, they should record this as sensitive data.

Examples of occasions when this type of information might be needed include: recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of pastoral duties.

Checklist for Processing Data

Before processing any personal data, all staff should consider the following checklist below:

- Do you really need to record the information?
- Is the information 'non sensitive' or is it 'sensitive' personal data?

- If it is sensitive, do you have the data subject's express consent?
- Has the subject been told that this type of data will be processed?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?
- The college will be able to justify processing the data if asked to do so?

5 Record-Keeping

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

- Accurate.
- Up-to-date.
- Fair.
- Kept and disposed of safely, and in accordance with the Data Retention Policy.

6 Manual Record

It is particularly important to ensure that manual records as well as computer–based records comply with the above requirements and to understand the sorts of manual records that are covered by the 1998 Act.

It should be noted that (with the exception of certain confidential references as noted in Section 9) all information held in manual records will need to be disclosed to an individual who makes a request for access to information under the Act. It is essential therefore that all statements made about an individual are written in a way that is fair and accurate. In particular staff should ensure that no libellous statements are made, which could result in legal action. Personal notes written about an individual in any form (even on a post-it note) would need to be disclosed if they are retained in a filing system.

7 Security

All staff are responsible for ensuring that any personal data which they hold is kept secure. Personal information should, so far as possible, be:

- Kept in a locked filing cabinet; or
- In a locked drawer; or
- If it is computerised, be password protected or encrypted; or
- Kept only on disk which itself is kept securely.

It is recognised that it is impractical for manual information to be locked away at all times during the working day, and that normal practice would be for filing cabinets and drawers to be unlocked during the day and locked overnight. It is nevertheless important to ensure that information is not accessible during the day to those who should not be permitted to see it. Staff who process personal data at home or other locations must take reasonable precautions to ensure that the data is kept securely and is not accessed, disclosed or destroyed. Staff using a home ipad, phone or laptop should ensure that they have up-to-date virus-scanning programming installed and password protected access.

Laptop computers should be kept constantly in view when travelling.

When personal data is to be destroyed, paper or microfilm records should be disposed of by shredding or incineration; computer hard disks or floppy disks should be re-formatted, over-written or degaussed.

8 Disclosure of Data

Staff must not disclose personal data to anyone except as required within the course of their duties. All staff are responsible for ensuring that personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure may be a disciplinary matter.

9 Confidential References

Confidential references written by external referees **received by** members of the college's staff are required to be disclosed to the individual who is the subject of the reference. However, they will generally only be disclosed either with the referee's consent or (providing they can be made anonymous, or with the writer's consent). A decision on whether to disclose a reference will be made by the college Principal.

Confidential references **written and held by** a member of staff, the author or within the author's area about a student or a member of staff and sent to an external individual or body are not disclosable by the college. (NB the individual who is the subject of the reference may ask for the reference to be disclosed by the receiver of the reference.)

10 Photographs and Videos

Where it is wished to take photographs or make video recordings of staff and/or students, as individuals, as small groups or organised groups, the individual staff members and the parent(s)/guardian(s) of the student(s) concerned should be informed of the purpose(s) and asked to give written consent. For general photographs or video recordings of campuses and public places, consent is not required.

11 The Internet and World Wide Web

Staff/Student Personal Data on the College's Website

Personal data placed on the college's website and made available via the Internet on the World Wide Web will be available in countries which do not have a data privacy regime considered adequate by the EU. Where it is wished to make staff and/or students personal data available in this way, as part of the normal organisational functioning and management of the institution, the staff and/or students concerned should be informed that they have the right to object to the use of their data where it would cause them significant damage or distress.

Where personal data is to be used for other purposes, for example publicity photographs, the consent of the staff and/or the parent(s)/guardian(s) of student(s) concerned must be obtained.

Collecting Personal Data

Sometimes Web pages are used to collect personal data, such as names and addresses of individuals who request college information, or who are registering to attend an open day. The relevant Webpage should indicate the purpose for which the data is collected, the recipients to whom it may be disclosed and an indication of the time period for which it will be kept (eg "while we process your application", rather than a specific date).

Individuals must be given the opportunity to opt out of parts of the collection or use of the data not directly relevant to the specific purpose.

12 Requests for Access to Information

Requests for access to information by staff, students and other data subjects must be handled in line with the college's Data Protection Policy.

APPENDIX 3 - GUIDELINES FOR STAFF – MANUAL RECORDS

1 Introduction

The 1998 Act extends the definition of 'data' from that held in computer-based systems to include all information recorded manually as part of a 'relevant filing system'. A relevant filing system is defined as a system where the records are structured, either by reference to individuals or by reference to criteria relating to individuals, so that "specific information relating to a particular individual is readily accessible". It needs to be borne in mind that guidance from the Information Commissioner indicates that this definition will be interpreted broadly.

It is not possible to be clear how this definition will translate in practical terms in all conceivable situations. This note attempts to indicate the types of records likely to come within the scope of the Act. The key elements of the definition of a relevant filing system are that the records will have a **structure** and be **readily accessible**.

The **structure** may work by one of two mechanisms:

(i) by reference to the individual by name or an identifying number or code, or
(ii) by reference to criteria related to individuals, e.g. year of course for a student, type of job for a member of staff.

To be **readily accessible,** it should be possible to locate information easily by virtue of the structure

2 Filing systems that would fall within the definition include:

Any system organised by:

- The surname of an individual.
- The enrolment number of a student.
- Staff number.
- Lists of staff arranged by job title.
- Lists of students by name or number giving assessment/examination marks.
- Identifying stickers.

The system may be:

- A card index.
- Information contained in a single file or in a section within a single file.
- Files contained in one or more drawers of a filing cabinet or desk.
- Files contained in one or more filing cabinets, in one or more offices.

Information about a particular student may thus be dispersed over different locations across the college, for example in:

- Central areas such as the Payroll Office.
- College's main office, Principal's office, SLT office(s), library or careers office.
- Learning Managers' offices.
- Safeguarding Officer's office.
- Departmental office(s).
- VMG tutor's room.
- The staffroom of individual members of staff.

3 Information that would not be covered would include

- A file of occasional correspondence on a particular topic, for example queries about field trip expenses, where correspondence is filed in date order and there is no way of knowing which individuals might have communicated with the college.
- Notes made by members of staff which are kept loosely on desks or in desk drawers, so long as these are not then placed within a structured filing system. Staff should, however, bear in mind the need to keep information securely.

APPENDIX 4 - GUIDELINES FOR STAFF – COMPUTER RECORDS

1 Introduction

Under the Act, although there is a broad interpretation of manually stored personal data: staff should treat ALL personal data stored on a computer system as subject to the Act. This means that it should adhere strictly to all of the eight principles given on page 1 of this policy. In particular, you should be aware of the following points:-

2 Access to data

Never give out personal data to any person not authorised to access it. This includes telephone numbers, academic details, addresses etc. If you wish to use any data for such general processes as research or reports that will be widely distributed, be absolutely certain that no individuals can be identified.

Seemingly innocuous requests, such as a student seeking the phone number of friend, should be refused. This also applies to parents: in particular details of one parent such as telephone number and address should not be given to the other or even to the student. This is particularly important where parents are separated.

3 Storage of data

Users should not have ANY files (e.g. word documents, spreadsheets, emails etc.) on either the network server, your hard disk, portable memory storage or your internet email page, that contain information about a third party that you would not be happy for them to see.

Regardless of this first principle, any information that is contained should be factual and verifiable and not be opinion or hearsay. Data must never be stored or disseminated in any way whereby non authorised persons may access it, for example on a shared network drive.

If you are in doubt, delete the file. It is good practice to delete those files that you will not need in electronic form. Any person can formally request to see any files that contain information relevant to them: deleting them after such a request is made is an offence under the data protection act. Note that data stored on a disc or memory devices is NOT deleted by simply pressing delete – the disk must either be reformatted, de-gassed or a 'secure delete' programme used.

Do not pass 'old discs' or memory devices on which have contained personal data and not been processed by one of these methods.

Remember that although your area of the network is nominally private to you, it is accessible by authorised network managers, technicians from outside, web hosting agencies, maintenance contractors etc. We have rigorous security procedures in operation to keep out unauthorised access, but our network is connected to the Internet: as you are probably aware from the press, intruder access through even the best security still occurs.

4 **Security of data**

Users are obliged to take all reasonable steps to minimise unauthorised access to information stored on the network. There are several simple but basic rules that MUST be adhered to at all times.

- NEVER let anybody know your passwords or identity: don't type passwords while you are being watched and if you must write it down, code it in some way and disguise its purpose. Obviously keep the note secure, but if you even suspect that somebody knows your access details, change your password immediately.
- Check that your screen cannot be seen easily through an open door, window etc.: if it can: reposition it!
- Never leave a logged in station unattended even for a few minutes. Even if you have only to 'pop out of the office for a few minutes' you should log out, however this isn't always realistic. To ensure security all stations MUST have a password protected screensaver enabled to operate after a few minutes. If in doubt of how to do this, ask.
- Never under any conditions give out personal details to ANYONE not on the staff of the college unless you are absolutely clear that this has been authorised, preferably in writing, if in doubt ask. If you are in any doubt whatsoever check with the registered data controller or your Principal.

Staff should NEVER copy personal student or staff data on to portable memory devices without the express permission of their line manager as they have justified that they have a genuine requirement for this data. In addition, the portable memory device MUST be securely encrypted with a password.

APPENDIX 5 - Privacy Notice for the College Workforce Employed or Otherwise Engaged to Work at HUTC

Privacy Notice – Data Protection Act 1998

Humber UTC is the Data Controller for the purpose of the Data Protection Act.

Personal data is held by the college about those employed or otherwise engaged to work at the college. This is to assist in the smooth running of the college and/or enable individuals to be paid. This personal data includes some or all of the following: identifiers such as name and National Insurance Number; characteristics such as ethnic group; employment contract and remuneration details; qualifications; and absence information.

The collection of this information will benefit both national and local users by:

- Improving the management of the college workforce data across the sector.
- Enabling a comprehensive picture of the workforce and how it is deployed to be built up.
- Informing the development of recruitment and retention policies.
- Allowing better financial modelling and planning.
- Enabling ethnicity and disability monitoring.
- Supporting the work of the college Teachers Review Body.

We are required to pass on some of this data to the Department for Education.

If you require more information about how the Department for Education store and use this data please contact them at the address below.

Public Communications Unit
Department for Education
Sanctuary Buildings
Great Smith Street
London
SW1P 3BT
Website: www.education.gov.uk

Email: info@education.gsi.gov.uk
Tel: 08700002288

We will not give information about you to anyone outside the organisation of the Department for Education without your consent unless the law and our rules allow us to. The exception to this is the publication of salaries of Principal and CEO, Executive Principals, Principals, Vice Principals, Assistant Principals and Directors of resources e.g. Finance and Human Resources.

APPENDIX 6 - Disclaimer

Data Protection and Confidentiality

Any information you give us via this website may be added to our database and will be processed in accordance with the Data Protection Act 1998.

We will never sell, rent or otherwise provide your personally identifiable information to any third parties (excluding those organisations that carry out functions or services on our behalf) unless you give us permission to do so, or we are obliged or permitted by law to disclose it or where it is necessary for the purpose of or in connection with legal proceedings or in order to exercise or defend legal rights.

All email messages sent to or from the college may be monitored to ensure compliance with internal policies and to protect our business.

Cookies and log files

Like most websites, the college website may use cookies and web log files to track site usage. A cookie is a tiny data file which resides on your computer and allows us to recognise you as a user when you return to our site using the same computer or web browser.

Due to the communication standards on the Internet, when you visit our website we may automatically receive a URL of the site from which you came and the site to which you are going when you leave our site.

We may also receive the Internet Protocol (IP) address of your computer (or the proxy server you use to access the World Wide Web), details of your computer systems and the type of web browser you are using, as well as the name of your ISP.

The information is used to analyse overall trend to help us improve our service, but is not linked to personally identifiable information in any way.

APPENDIX 7 - Fair Processing Notice

Humber UTC processes personal data about its students and is a "data controller" in respect of this for the purposes of the Data Protection Act 1998. It processes this data to:

- Support its students' teaching and learning.
- Monitor and report on their progress.
- Provide appropriate pastoral care, and
- Assess how well the college as a whole is doing.

This information includes contact details, national curriculum assessment results, attendance information, characteristics such as ethnic group, special educational needs and any relevant medical information.

From time to time, the college is required to pass on some of this data to local authorities, the Department for Education (DfE) and to agencies that are prescribed by law, such as the Qualifications and Curriculum Authority (QCA), Ofsted, the Department of Health (DH) and Primary Care Colleges (PCT). All these are data controllers for the information they receive. The data must only be used for specific purposes allowed by law.

The **Local Authority** (LA) uses information about children for whom it provides services to carry out specific functions for which it is responsible, such as the assessment of any special educational needs the child may have. It also uses the information to derive statistics to inform decisions on (for example) the funding of colleges, and to assess the performance of colleges and set targets for them. The statistics are used in such a way that individual children cannot be identified from them.

The **Qualifications and Curriculum Authority (QCA)** uses information about students to administer the national curriculum assessments portfolio throughout Key Stages 1 to 3. This includes both assessments required by statute and those that are optional. The results of these are passed on to DfE to compile statistics on trends and patterns in levels of achievement. The QCA uses the information to evaluate the effectiveness of the national curriculum and the associated assessment arrangements, and to ensure that these are continually improved. www.qca.org.uk
Data Protection Officer, QCA, 83 Piccadilly, LONDON, W1J 8QA.

Ofsted uses information about the progress and performance of students to help inspectors evaluate the work of colleges, to assist colleges in their self-evaluation, and as part of Ofsted's assessment of the effectiveness of education initiatives and policy. Ofsted also uses information about the views of children and young people, to inform children's services inspections in local authority areas. Inspection reports do not identify individual students.
www.ofsted.gov.uk.
Data Protection Officer, Alexandra House, 33 Kingsway, London WC2B 6SE;

Primary Care Trusts (PCT) use information about students for research and statistical purposes, to monitor the performance of local health services and to evaluate and develop them. The statistics are used in such a way that individual pupils cannot be identified from them. Information on the height and weight of individual pupils may however be provided to the child and its parents and this will require the PCTs to maintain details of students' names for this purpose for a period designated by the Department of Health following the weighing and measuring process. PCTs may also provide individual colleges and LAs with aggregate information on students' height and weight.
http://www.nhs.uk/England/AuthoritiesColleges/Pct/Default.aspx

The **Department of Health (DH)** uses aggregate information (at college year group level) about students' height and weight for research and statistical purposes, to inform, influence and improve health policy and to monitor the performance of the health service as a whole. The DH will base performance management discussions with Strategic Health Authorities on aggregate information about pupils attending colleges in the PCT areas to help focus local resources and deliver the Public Service Agreement target. The Department of Health will also provide aggregate PCT level data to the Healthcare Commission for performance assessment of the health service. www.dh.gov.uk
Data Protection Officer at Skipton House, 80 London Road London SE1 6LH;

The **Department for Education (DfE)** uses information about students for research and statistical purposes, to inform, influence and improve education policy and to monitor the performance of the education service as a whole. The DfE will feed back to colleges information about their students for a variety of purposes that will include data checking exercises, use in self-evaluation analyses and where information is missing because it was not passed on by a former college.
Data Protection Officer, DfE, Sanctuary Buildings, Great Smith Street, London, SW1P 3BT

Students, as data subjects, have certain rights under the Data Protection Act, including a general right of access to personal data held on them. If you wish to access your personal data, or you wish your parents to do so on your behalf, then please contact the college Principal in writing.

Approved By:
Date:

Description of Data to be Removed:

Reason for Data to be Removed:

APPENDIX 8 – Authorisation to Remove Sensitive Data from the College

Approved By:
Date:

Description of Data to be Removed:

Reason for Data to be Removed:

Method by which Data will be Securely Stored:
Name:
Job Title:

Approved By:
Date:

Description of Data to be Removed:

Reason for Data to be Removed:

Method by which Data will be Securely Stored:

Approved By:
Date:

Description of Data to be Removed:

Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. In a college context this will include e.g. **names, contact details, gender, dates of birth, behaviour, academic achievements** as well as other sensitive information e.g. religious beliefs, physical and mental conditions and racial or ethnic origins.

Therefore you must:

- Treat personal data with care and remember that you have a duty of confidentiality towards the Data Subject. All paper copies of personal information should be kept in a locked filing cabinet or cupboard which should only be accessed by authorised personnel on a need to know basis.
- Only disclose personal information to those authorised in your Data Protection notification to the Information Commissioner.
- Ensure that personal data is not left on your desk in view of others. Lock it away when not in use.
- Logoff/Lock PCs/Laptops while you are away from them for lengthy periods.
- Ensure that your PC/Laptop is password protected.
- Do not share your Logon with any other person.
- Don't tell anyone else your password.
- Ensure no one else, especially students or members of the public, can read information from your computer screen. No one should be able to view data without authorisation.
- Do not store personal data on removable media (e.g. USB stick, CD ROM) unless fully encrypted and authorised by the Principal.
- Do not remove personal data (removable media/laptop/file) from college premises unless appropriately stored and authorised by the Principal.
- Don't use unauthorised software on your PC/Laptop.
- Back-up media should be kept in a secure storage area.

If in doubt, seek further advice.