1. Introduction

Plumpton College holds information about its Corporation members, employees, students, partners, suppliers and other users as a normal part of its day-to-day business. It is necessary for example to process information so that staff can be recruited and paid, students enrolled, courses organised, examinations and assessments held and legal obligations to funding bodies and Government complied with.

The aim of the Data Protection Act 1998 ("the Act") is to ensure that data is collected and used in a responsible and accountable manner and to provide the individual with a degree of control over the use of their personal data. To comply with the law information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The Act also allows individuals to obtain a copy of their own data, the right to have inaccurate personal data corrected or erased and, where appropriate, to seek redress for any damage caused. The Act obliges the College to provide a complete description of all personal data held by the College, their uses, purposes, disclosures and sources, to the Information Commissioner's Office. The Act provides for criminal offences if its obligations are neglected.

The purpose of this document is to make all staff and students aware of their responsibilities towards all personal data held by the College and to indicate the practical steps taken to comply with the Act.

2. The Data Protection Act 1998

The 1998 Act places duties and obligations on "Data Controllers" in relation to their "processing" of "personal data". *Personal data* includes information about living, identifiable individuals (data subjects) that is to be processed by means of automated equipment (including computer processing and CCTV images). This may include e-mails which are processed with reference to the data subject.

Personal data also includes information recorded as part of a "relevant filing system". This is any manual filing system, microfiche or paper set of information that is structured in such a way that information relating to a particular individual is readily accessible.

Processing means obtaining, recording, holding, organising, altering, retrieving, consulting, destroying or carrying out any operation on the information or data.

The eight Data Protection Act Principles provide the framework for processing. Broadly these state that personal data must be:

1. fairly and lawfully obtained and processed
2. held and processed for limited purposes
3. adequate, relevant and not excessive
4. accurate and where necessary kept up to date
5. held for no longer than is necessary
6. processed in accordance with individuals' rights
7. secure
8. not transferred to countries without adequate protection (outside EEA)

Rights for Individuals under the Data Protection Act 1998:

- right of subject access (to data held on computer records and relevant filing systems upon making a request in writing and paying a fee)
- right to prevent processing likely to cause unwarranted and substantial damage or distress
- right to prevent processing for the purposes of direct marketing
- right to compensation
- right to correction, blocking, erasure or destruction
- right to ask the Information Commissioner to assess whether the Act has been contravened

Criminal Offences under the Data Protection Act 1998:

- processing without notification
- failure to comply with an enforcement notice
- unlawful obtaining or disclosure of personal data
- selling or offering to sell personal data without the consent of the data subject

3. Status of the Policy

This policy is a broad summary of Plumpton College's responsibilities under the Data Protection Act. 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 failures to follow the policy can therefore result in disciplinary proceedings.

4. Plumpton College Compliance Framework

The College, as a body corporate, is the Data Controller under the Act and the Corporation is therefore ultimately responsible for implementation.

The Data Protection Officer on behalf of the College is the Deputy Principal.

The main duties of the Data Protection Officer are to:

- ensure that the College's notification under the Act is accurate and kept up to date
- act as an interface between the College and the Information Commissioner
- ensure that the data protection policy is up to date
- act as an initial contact point for Subject Access requests and co-ordinate formal replies
- co-ordinate requests for information from external bodies (e.g. Police, DSS, Inland Revenue, Local Authorities)
- provide training on Data Protection issues
- carry out regular audits of each Department
- ensure up-to-date records of all computerised data and all manual data are held in structured filing systems, including details of the personnel authorised to access the data.
- develop and implement adequate retention policies for all Personal Data
- ensure that appropriate contracts are in place with third parties who handle Personal Data on behalf of the College
- ensure that all processing of information provides details as to the purpose(s) for which the data will be processed and if necessary consent to that processing is provided by the Data Subject
- ensure adequate safeguards are in place against disclosure to unauthorised persons and/or for unauthorised purposes
- ensure that effective procedures are in place to identify individuals who do not wish to receive direct marketing material.

A copy of this Data Protection Policy will be placed on the Q drive and on the website.

The College will maintain a register of all systems used to process personal data in the College. This will include the type of system, the types of a personal data held and the purpose of processing. The purpose of the register is to ensure that all processing of personal data within the College is adequately notified to the Information Commissioner. A copy of the College's registration is available for reference in the Resources Centre. College staff are only allowed to use authorised systems for processing personal data. Any request to establish new systems or change existing systems for processing personal data must be made formally to the Data Protection Officer.

5. Responsibilities of Staff

Staff are expected to:

- Familiarise themselves and comply with the Data Protection Policy.
- Ensure that any data which they propose to process is covered by the College's Data Protection Registrations.
- Observe strict control of all databases of information on individuals, whether they be staff, students, or members of the general public.
- Ensure that an indication of the purpose(s) appears on any form used to collect data and, where necessary, an explanation is given as to why personal

data is being collected.

- Ensure that personal data obtained for one stated purpose is not used for a completely different purpose without the individual being informed of the different purpose.
- Ensure that any personal data kept is accurate, held securely and disposed of in a timely and secure manner.

The College must register all databases or it could face legal action.

- Failure of any member of staff to inform College management of a database could result in disciplinary action.
- The holding of a College-related database outside the College also falls within these restrictions.

6. Responsibilities of students

The College requires all students to consent to processing under the Data Protection Act and to comply with the Data Protection Policy.

7. Responsibilities of Contractors and Partners

A data protection memorandum of understanding will be included in all contracts where third parties process data on behalf of Plumpton College and where third parties have access to data as a necessary part of their contracted work.

8. Notification of Data Held and Processed

Employees, students, Corporation Members and other users of the College have subject access rights to certain personal data that is held about them either on computer or in manual files. They are entitled to know:

- what information the College 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 Act

9. Subject access rights to information

All data subjects should be informed that they have the right to access their data. They should be told how they can exercise their right to access the data.

The formal procedure for controlling and processing Subject Access Requests is cumbersome. Wherever possible, the informal disclosure of personal data to data subjects is encouraged, particularly where administrative gains may result - for

example, for the periodic confirmation of the accuracy of personal details, such as current address and so on. However, where an informal approach is adopted, it is essential that the Data Protection Principles and College's procedures are fully observed.

All formal subject access requests must be made using the College's Subject Access Request Form (Appendix A), which should be forwarded immediately to the Data Protection Officer.

The data subject must return the form with sufficient information to enable the College to locate the information that the subject seeks. The College is not obliged to comply with open ended requests. The College may refuse to disclose data that makes reference to the personal data of third parties.

The College will make a standard charge of £10 on each occasion that access is requested, although the College has the discretion to waive this charge.

After an acknowledgement letter is sent to the applicant, the Data Protection Officer will forward a copy of the request to the relevant Head of Department requiring the retrieval of the data by a specific date. The results of the retrieval must be returned to the Data Protection Officer in a sealed envelope, marked "Staff in Confidence", by the specified date. "Nil" returns are also required.

The Data Protection Officer will co-ordinate the formal reply to the applicant, or will advise them that no Personal Data relating to them is held.

10. Disclosure of personal data

Personal data must not be disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party. Particular discretion must be used before deciding to transmit personal data by fax or email.

Where non routine requests are made or where staff are unsure of their responsibilities they should seek the advice of their line manager. The Data Protection Officer should be consulted when necessary.

All requests for disclosure of Personal Data from persons outside the College must be treated with caution by all staff.

- Personal Data must not be disclosed to an external body over the telephone. Individuals making such enquiries should be asked why the information is required and be informed of the College's requirement to comply with the Act. Wherever possible the Data Subject should be informed of the enquiry to enable them to respond directly.
- Parents, relatives and guardians should be informed of the College's requirement to comply with the Act if making representation on behalf of a student or employee.

- Personal Data requested by members of staff from other areas of the College should only be released when it has been established that the information required is necessary for them to carry out their official duties.
- All requests from outside agencies such as the Police, DSS, Inland Revenue, Local Authorities, Overseas Embassies or High Commissions should be submitted in writing and forwarded to the Data Protection Officer.

Staff should be aware that those seeking information about individuals may use deception to obtain information. Staff should take steps to verify the identity of those seeking information, for example by obtaining the telephone number and returning the call or by reviewing identification documents if an application is made in person. All applications for data should be made in writing.

Where a disclosure is requested in an emergency, staff should make a careful decision as to whether to disclose, taking into account the nature of the information being requested and the likely impact on the subject of not providing it.

10.1 Disclosure of Data to Employers

Many students attend College under the sponsorship of their employers. This may include paid time to attend or payment of fees. These students will be required to consent to the sending of routine reports to their employers on academic progress and attendance.

10.2 Disclosure of information to students' parents or guardians

Students are private individuals and the College has no responsibility or obligation to keep relatives informed of progress or any other aspect of studies or private life. Although staff may come under pressure to discuss students' cases with parents, it is essential that personal information is not disclosed without the written consent of the student involved.

The College may inform parents / guardians of students who are under 18 of any concerns regarding serious academic, behavioural or financial issues.

Other non routine requests for information from parents or guardians of students under 18 should be considered carefully. It should be normal procedure to request permission from the student before disclosing any additional information.

For students over 18 or who become 18 during their course and are not totally independent (defined as living independently from parents / guardians for a period of over two years) the College may inform parents / guardians of any serious academic, behavioural or financial issues unless specifically requested not to do so in writing by the student and parent / guardian.

Regardless of age, the College will inform the next of kin if any serious accident occurs.

11. 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 student onto any course, and a condition of employment for staff.

Some jobs or courses will bring the applicants into contact with children, including young people below the age of 18. The College has a duty to ensure staff 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 make sure employees and those who use the College facilities do not pose a threat or danger to other users. Where appropriate therefore the college will obtain information about previous criminal convictions.

The College will notify all users at the point where information is collected from them which information will be processed and the purpose of processing under the Data Protection Act. The consent of the user will be obtained at the point of collection. This includes:

- Application forms for Corporation members
- Application forms for staff
- Application forms for students
- Learning agreement forms

Retrospective consent will be sought where necessary.

The College provides a statement to all enrolling students regarding those organisations with whom personal information will be shared and undertaking that no personal information will be passed to organisations for marketing or sales purposes. At the same time students are invited to specify if they do not wish to be contacted by the ESFA or its partners in respect of surveys and research or regarding courses or learning opportunities.

The College will circulate data periodically to data subjects to provide opportunity for data to be updated and corrected.

12. Processing sensitive information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender or family details. This may be to ensure the College is a safe place for everyone, or to operate other College policies, such as the absence policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern, 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.

13. Publication of College information

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

- Names of Corporation Members and register of interests
- Names and positions of senior post holders and register of interests
- Staff register of interests

Any individual who has good reason for wishing details to remain confidential should contact the designated Data Protection Officer.

14. Data Security

All staff are responsible for ensuring that:

- Any personal data, which they hold, is kept securely
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party
- Checking carefully the identification of any person making a request for information
- Personal information is kept in a locked filing cabinet or locked drawer
- If personal information is computerised, it is password protected
- Only authorised access to computers is allowed (eg by not disclosing passwords)
- Passwords are changed at regular intervals
- Computers are switched or logged off when not in use
- Doors to rooms containing computers are locked when not in use
- Care is taken with data held on portable disks or laptop computers
- Casual disclosure does not take place by for example leaving computer printouts or manual records uncovered on desktops or by allowing unauthorised users to view computer screens
- Keeping computer printouts securely and destroying them in a confidential manner.
- College hardware or software is not removed from the College without prior authorisation

The removal of College-related personal data on a computer to offsite locations or the holding of College-related personal data on a computer outside the College will only be permitted in strictly controlled circumstances. It is not permitted to hold any College-related data off-site either on a College-owned or personal computer without prior approval.

Unauthorised disclosure may be regarded as a disciplinary matter, and may be considered gross misconduct in some cases.

15. Retention of data

Personal data will be retained for no longer than is necessary for the purpose for which it was collected. Standard retention times are necessary to meet various contractual requirements. Standard retention times for finance related documents are specified in the College Retention of Documents Procedure (Appendix B).

16. Disposal of data

Particular care must be taken with the disposal of personal data. Staff should be aware that the same standards should be applied to informal records, lists and printouts held by individual members of staff containing personal data as to records which are part of the formal College records system. This material must not be disposed of in ordinary office waste paper bins. Personal data must be destroyed by secure methods such as shredding.

Electronically held data time expires after the same period as hard copy. Staff should therefore delete this information at the earliest opportunity after the anniversary of the date of disposal.

17. Examination results

Students will be entitled to information about their marks for both coursework and examinations. Examination results are normally notified directly to students. Lists of examination results identifying individual students are not posted on College notice boards. News stories focussing on individual students will only be made available with the consent of the student.

18. References

The provision of a reference will generally involve the disclosure of personal data. The College is responsible for references given in a corporate capacity. All staff references requested should be referred to the Principal.

The College is not responsible for references given in a personal capacity. These should never be provided on Plumpton College stationery and should be clearly marked as personal.

The College will not provide subject access rights to confidential references written on behalf of the College about employees and students and sent to other organisations. This is a specific exemption allowed by the Act.

The College recognises that once the reference is with the organisation to whom it was sent then no specific exemption from subject right access exists.

The College will normally provide subject right access to confidential references received about employees and students provided to the College by other organisations. However the College may withhold information if it is likely to result in harm to the author or some other person or if it reveals information about another third party other than the previous supervisor or manager of the employee.

19. CCTV

CCTV systems in the College are only used for the prevention and detection of crime. CCTV systems must be positioned to avoid capturing images of persons not visiting College premises. The recorded images must be stored safely and only retained long enough for any incident to come to light. Recordings will only be made available to law enforcement agencies involved in the prevention and detection of crime and to no other third party. Staff who are involved in the management of CCTV systems will ensure that they abide by the following code of practice:

- All recorded images will be of good quality and factually correct.
- Copies of CCTV forage will be marked with a unique serial number.
- Only authorised personnel from enforcement agencies will be permitted to view video images within the Control Room (Student Services Office).
- Only Student Services staff will be permitted to operate the equipment within the CCTV Control Room.
- Any investigating officer will be required to sign a release certificate for any images removed from the Control Room so that a clear audit trail of evidence is maintained.
- All images recorded within the Control Room not required for investigation of, or prosecution of, an offence, will be destroyed after 31 days.
- Images may be retained longer than 31 days but only at the request of an enforcement agency to continue an inquiry or for a prosecution.
- Any investigating officer who signs out a copy tape or still image will receive a chaser letter at regular intervals requesting the image's return.
- No unauthorised access to images held within the Control Room will be permitted.
- The Duty Operator will be responsible for the security of the images held within the Control Room.
- All images recorded by the CCTV cameras will have the date, time and location of the camera providing the images clearly superimposed on them.
- All equipment within the Control Room including cameras, video recorders and time generators will be checked daily and faults reported and repaired as quickly as possible.
- Operators will not use the cameras to follow individuals because of their race, sex, colour, dress or appearance. Nor will they stereotype members of the public.
- No images of any kind produced by College's Control Room will be released for entertainment purposes.

- To ensure the production of the highest quality images a full maintenance programme will be put in place.

20. Direct Marketing

The College will only use other personal data (including photographic images) for promotional campaigns or to market additional activities to existing or previous students where they have given consent. Any staff wishing to send out marketing material to students such as details for further course opportunities must check that the student has consented.

Approved By: Corporation
Date of Approval: 3rd October 2017
Frequency of Review: Every Three Years
Date of Next Review: October 2020

The SMT is delegated to approve minor changes to the policy in response to legal changes and best practice.

DATA PROTECTION ACT 1998

SUBJECT ACCESS REQUEST

This form is to be completed by an individual who seeks access to personal data held about them by Plumpton College

To help the College comply with your request please give accurate personal details and an indication of the kind of data you are looking for.

Plumpton College charges a fee of £10.00 per subject access request. The College will try to provide the data you seek within 40 calendar days of receipt of your request, but will contact you if we are not able to meet your request with the target timescale. Copies of two items of proof of identity e.g. birth certificate, passport must be included.

SURNAME	FIRST NAME(s)	D.O.B.	GENDER

CURRENT ADDRESS:	ADDRESS: (at time of Plumpton College contact)

REQUEST: (please indicate)

STAFF ☐ **STUDENT** ☐ **OTHER** ☐

START DATE	FINISH DATE	COURSE TITLE/JOB TITLE	

DESCRIPTION OF DATA REQUIRED:

I enclose a cheque to the value of £10.00 payable to Plumpton College ☐

I enclose proof of personal identity ☐

Signed …….. Date ……

Please return this form to the Director of Finance & Administration, Plumpton College, Ditchling Road, Plumpton, East Sussex, BN7 3AE

For Office Use Only

Date Received by Plumpton College: ……	Date Data Supplied: ……

Appendix B

Guidelines for Retention of Personal Data

Note: This is not an exhaustive list. Medical records, for example, are kept for a variety of health and safety reasons and will carry their own retention times.

Type of Data	Suggested Retention Period	Reason
Personnel files included in training records and notes of disciplinary and grievance hearings.	6 years from the end of employment	References and potential litigation
Application forms/interview notes	At least 6 months from the date of the interviews	Time limits on litigation
Facts relating to redundancies where less than 20 redundancies	3 years from date of redundancies	As above
Facts relating to redundancies where 20 or more redundancies	12 years from date of redundancies	Limitation Act 1980
Income Tax and NI returns, including correspondence with tax office	At least 6 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	At least 6 years after the end of the financial year to which the records relate	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	At least 6 years after the end of the financial year to which the records relate	Statutory sick Pay (General) Regulations 1982
Wages and salary records	At least 6 years after the end of the financial year to which the records relate	Taxes Management Act (1970)
Accident books, and records and reports of accidents	6 years after the date of the last entry	RIDDOR 1985
Health records	During employment	Management of Health and Safety at Work Regulations
Health records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical Records kept by reason of the Control of Substances Hazardous to Health Regulations 1994	40 years	COSHHR 1994
Student records, including academic achievements, and conduct	At least 6 years from the date the student leaves College, in case of litigation of negligence. For EU Funded projects records should be kept for 7 years after completion of programme. At least 10 years for personal and academic references, with the agreement of the student.	Limitation period for negligence