Data Protection Policy and Procedure

INTRODUCTION

West Nottinghamshire College is committed to preserving the privacy of its students and employees and to complying with the Data Protection Act 1998. To achieve this commitment information about our students, employees and other clients and contacts must be collected and used fairly, stored safely and not unlawfully disclosed to any other person.

Information that is already in the public domain is exempt from the Data Protection Act 1998. 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 our Governors.
- Photographs of key staff (i.e. members of the Executive and other managers) with the consent of the individual
- List of staff.
- Learner performance data.

PRINCIPLES

The College, its staff and others who process or use any personal information must ensure that they follow the data protection principles set out in the Data Protection Act 1998. These are that personal data shall:

- Be obtained and processed fairly and lawfully.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept longer than is necessary for that purpose.
- Be processed in accordance with the data subject rights.
- 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 will not release staff or learner data to third parties except to relevant statutory bodies. In all other circumstances the College will obtain the consent of the individuals concerned before releasing personal data.

RESPONSIBILITIES

Corporation Board

The Corporation Board are responsible for the oversight and implementation of this policy.

The Principal and Senior Managers

It will be the responsibility of the Principal and senior managers to ensure compliance with the policy and for communicating the policy to all staff.

Data Protection Coordinator

The nominated Data Protection Coordinator for the College is the Head of ICT and Learning Resources – they have operational responsibility for the implementation of this policy.

Managers

All managers are responsible for ensuring that staff are aware of and abide by this policy.

All Staff

All staff are responsible for ensuring that any personal data which they hold is kept securely and personal information is not disclosed in any way and to any unauthorised third party.

All Students and Staff

Students and staff are responsible for ensuring that all personal data provided to the College is accurate and up to date.

COMPLIANCE

Failure to comply with the data protection policy and procedure could result in disciplinary action.

REVIEW

This policy and related procedures will be reviewed and issued on at least an annual basis.

Data Protection Procedure

1. INTRODUCTION

The College needs to keep certain information about its employees, students and other users to allow us to monitor recruitment, attendance, performance, achievements and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the College must comply with the Data Protection Principles, which are set out in the Data Protection Act 1998. In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- 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 staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the College has developed the Data Protection Policy, available on the Staff net.

The College will keep a register of staff authorised to access and process learner and staff data and these members of staff will be asked to agree a confidentiality statement on network login.

2. RESPONSIBILITIES OF STAFF

2.1 Information About Yourself

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, i.e. change of address.
- Informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed us of them.

2.2 Information About Other People

All staff must comply with the following guidelines:

All staff will process data about individuals 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 individuals give their consent to this type of processing, and are notified of the categories of processing, as required by the

Owner: Gavin Peake
Created on: May 2016
Review Date: May 2017

1998 Act. The information that 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.

Information about an individual's physical or mental health; sexual orientation; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with consent.

All staff have a duty to make sure that they comply with the data protection principles, which are set out in the staff handbook and the College 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 College policy.

The College will designate staff in the relevant area as 'authorised staff'. These staff are the only staff authorised to access data that is:

- Not standard data; or
- Sensitive data.

The only exception to this will be if a non-authorised member is satisfied and can demonstrate that the processing of the data is necessary:

- In the best interests of the individual or staff member, or a third person, or the College AND
- He or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances.
- This should only happen in very limited circumstances. E.g. an individual is injured and unconscious and in need of medical attention, or a member of staff tells the hospital that the individual is pregnant or a Jehovah's Witness.

Authorised staff will be responsible for ensuring that all personal data is kept securely. In particular staff must ensure that personal data is:

- Put away in lockable storage
- Not left on unattended desks or tables.
- Unattended ICT equipment should not be accessible to other users.
- ICT equipment used off-site must be password-protected.
- Data files on CD or memory stick or email attachments used off-site containing personal data must be password-protected.
- Paper records containing personal data must be shredded where appropriate.

Staff must not disclose personal data to any individual, unless for normal academic or pastoral purposes, without authorisation or agreement from the data controller, or in line with the College policy.

Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated data controller, or in line with the College policy.

Before processing any personal data, all staff should consider the following.

- Do you really need to record the information?
- Is the information 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the individual been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- 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 individual or the safety of others to collect and retain the data?

3. RIGHTS TO ACCESS INFORMATION

Staff, individuals and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the College Standard Request Form for Access to Data and send it to Customer Services. (Appendix 2), also located on the staff net. This request should be made in writing using the Standard Form to Access Data also located on the staff intranet.

The College will make a charge of £10 on each occasion that access is requested, although the College have discretion to waive this. This charge will be automatically waived for staff.

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

4. 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 an individual onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. The College has a duty under the Children Act and other enactment to ensure that staff are suitable for any job offered. The College also has a duty of care to all staff and students and must therefore make sure that employees and those who use the College facilities do not pose a threat or danger to other users.

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

Therefore, all prospective staff and students will be asked to sign either an appropriate HR form or an individual document regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such documents may result in the offer being withdrawn.

5. THE DATA CONTROLLER AND THE DESIGNATED DATA CONTROLLER/S

The College as a corporate body is the data controller under the Act, and the board is therefore ultimately responsible for implementation. However, the designated data controllers will deal with day-to-day matters.

The nominated Data Protection Coordinator is the Director of IT whose contact details can be found on the College's StaffNet in the College search area. In the event of the Director: IT unavailable, the nominated deputy for the Data Protection Coordinator is the Director: Human Resources.

The College's designated data controllers are the Director: Human Resources who is responsible for all data relating to staff and the Deputy Principal/Finance Director who is responsible for all data relating to students and finance.

6. RETENTION OF DATA

Please see appendix 1 for the guidelines for the retention of personal data.

7. NOTIFICATION OF CHANGES TO THE PROCESSING OF PERSONAL DATA

The existing Data Protection Register for the College can be found at https://ico.org.uk/esdwebpages/search

Any changes will be reflected on this site and notified in the first instance on the College StaffNet.

8. CONCLUSION

Compliance with the 1998 Act is the responsibility of all members of the College. Any breach of the data protection policy may lead to disciplinary action being taken, access to the College being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation of this policy should be referred to your line manager.

Appendix 1

GUIDELINES FOR RETENTION OF PERSONAL DATA

Appendix 2

Type of Data	Suggested Retention Period	Reason
Personnel files including 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 the date of redundancy	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 3 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	As Above	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	As Above	Statutory Sick Pay (General) Regulations 1982
Wages and Salary records	6 years	Taxes Management Act 1970
Accident books, and records and reports of accidents	3 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 the College, in case of litigation for negligence, At least 10 years for personal and academic references, with the agreement of the student.	Limitation period for negligence.

Owner: Gavin Peake
Created on: May 2016
Review Date: May 2017

STANDARD REQUEST FORM FOR ACCESS TO DATA

I……wish to have access to either:

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

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

    - Academic marks or course work details
    - Academic or employment references
    - Disciplinary records
    - Health and medical matters
    - Political, religious or trade union information
    - Any statements of opinion about my abilities or performance
    - Personal details including name, address, date of birth etc
    - Other information

(Please tick as appropriate)

3. Before releasing information we will require ID in the form of a photo ID or passport to confirm the information is being released to an authorised person.

I understand that I will have to pay a fee of £10.00 (Ten pounds)

Signed_____

Dated _____

Owner: Gavin Peake
Created on: May 2016
Review Date: May 2017