Data protection policy

Date ratified: 18th March 2020

Date policy due to be reviewed: March 2022

Committee responsible for policy: Board of Governance

DATA PROTECTION POLICY

The Ridge Employability College

This policy is connected to The Ridge Employability College's Safer Recruitment and Discipline at work policies, which provide guidelines on data collection, management and retention.

Introduction

The Ridge Employability College ('The College') needs to keep certain information about its employees, learners and other users to allow it to monitor such matters as 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 agencies complied with. To comply with the law, information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the college will comply with the Data Protection Principles which are set out in the Data Protection Act 2018 (the 2018 Act) and with the requirements of the Freedom of Information Act 2000. 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 and a printout of the data subject's data record provided to them every 12 months to check its accuracy.

• Not be kept for 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 will ensure that they follow these principles at all times. In order to ensure that this happens, The College has developed the following Data Protection Policy.

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 failures to follow the policy can therefore result in disciplinary proceedings. Any member of staff, learner or Director, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated data controller initially.

The Data Controller and the Designated Data Controllers

The college is the data controller under the 2018 Act, and is therefore ultimately responsible for implementation. However, the designated data controller will deal with day-to-day matters. This college's designated data controllers are the Board of Directors.

Authorised Staff

The college will designate staff in each area as 'authorised staff'. These staff members the only staff authorised to hold or process data that is:

• Not standard data; or

• Sensitive data.

The authorised staff members are Head of college, Data Manager, Curriculum Lead and Administration staff. The only exception to this will be if a non-authorised staff member is satisfied that the processing of the data is necessary:

• In the best interests of the learner 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 happen only in very limited circumstances (such as where a learner is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the learner is pregnant or a Jehovah's Witness). Authorised staff will be responsible for ensuring that all data is kept securely.

Notification of Data Held and Processed

All staff, learners and other users are entitled to:

• Know what information the college holds and processes about them and why.

• Know how to gain access to it.

• Know how to keep it up-to-date.

• Know what the college is doing to comply with its obligations under the 2018 Act.

The college will therefore provide all staff and learners and other relevant users with a standard form of notification by making this policy available on 365. Members of the public are also entitled to access information, subject to certain controls, under the Freedom of Information Act.

Responsibilities of Staff

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. Any gaps in employment history are to be rigorously checked.

• Informing the college promptly of any changes to information already provided (e.g.: changes of address).

• Checking the information (about information kept and processed about staff) that the college sends out from time to time.

• 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. If and when, as part of their responsibilities, staff collect information about other people, (e.g.: about learners' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they will comply with the guidelines for staff, which are at appendix 1.

Data Security

All staff members are responsible for ensuring that:

• Any personal data which they hold is kept securely.

• Personnel information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party. Staff should note that unauthorised disclosure will be a disciplinary matter, and may be considered gross misconduct.

Personal information will be:

• Kept in a locked filing cabinet; or

• In a locked drawer; or

• If it is computerised, be password protected; or

• Kept only on memory stick which itself is kept securely;

• Only kept away from college premises with prior written authorisation from an authorised officer and (where it is held on a computer) on college equipment.

Authorised Disclosures

The college will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the designated data controller may need to disclose data without explicit consent for that occasion. These circumstances are strictly limited to:

a. Learner data disclosed to authorised recipients related to education and administration necessary for the college to perform its statutory duties and obligations.

b. Learner data disclosed to parents/carers in respect of their learner's health, safety and welfare.

c. Learner data disclosed to parents/carers in respect of their learner's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the college.

d. Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.

Learner Obligations

Learners are expected to ensure that all personal data provided to the college is accurate and up-to date. They must ensure that changes of address, etc. are notified to the office, tutor or other person as appropriate.

Rights to Access Information

In accordance with the law, staff, learners and other users of the college have the right to access appropriate 'personal data' that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should write to the designated data controller. This request should be made in writing. 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 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.

Requests to access information from Learners

Requests from learners will be processed as any subject access request and the copy will be given directly to the learner, unless it is clear that the learner does not understand the nature of the request. Requests from learners who do not appear to understand the nature of the request will be referred to their parents/carers. Requests from parents/carers in respect of their own learner will be processed as requests made on behalf of the data subject (the learner) and the copy will be sent in a sealed envelope to the requesting parent/carer. With regard to requests from parents/carers in respect of their own learner who is over the age of 16, permission will be sought from the learner concerned and data will be sent in a sealed envelope to the requesting parent/carer only if such permission is granted.

Publication of College Information

It is the college's policy to make as much information public as possible. The college has lodged its registration details with the Information Commissioner's Office (ICO).

Subject Consent

In many cases, under the Data Protection Act, the college can process personal data only with the consent of the individual. In some cases, if the data is sensitive (e.g.: race or ethnic origin, physical or mental health), express consent must be obtained. Agreement to the college processing some specified classes of personal data is a condition of acceptance of a learner onto any course, and a condition of employment for staff. This includes information about previous criminal convictions. Some work placements or courses may bring the applicants into contact with young people between the ages of 14 and 18. The college has a duty under the Children Act and other enactments to ensure that staff members are suitable for the job, and learners for the courses offered. The college also has a duty of care to all staff and learners 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 use the information only in the protection

of the health and safety of the individual, but will need consent to process it (e.g.: in the event of a medical emergency).

Processing Sensitive Information

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

Retention of Data

The college will keep some forms of information for longer than others. Because of storage limitations, information about learners cannot be kept indefinitely, unless there are specific requests to do so. In general, information about learners will be kept for a maximum of seven years after they leave the college.

This information will include:

• Names and addresses

• Academic achievements, including marks for coursework and

• Copies of any reference written.

In general, all information about staff will be kept for seven years after a member of staff leaves the college. Some information, however, will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. It is the duty the of the designated data controller to ensure that obsolete data is properly erased.

Conclusion

Compliance with the 2018 Act is the responsibility of all members of the college. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to college facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated data controllers.

Review

This policy will remain in force until amended or withdrawn by the college after consultation with staff.

APPENDIX 1

Staff Guidelines for Data Protection

1. Staff will process data about learners on a regular basis, when marking registers, or college work, writing reports or references, or as part of a pastoral or academic supervisory role. The college will ensure through registration procedures that all learners give their consent to this sort of processing, and are notified of the categories of processing, as required by the 2018 Act. The information that staff members 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 learner's physical or mental health (e.g.: recording information about dietary needs, for religious or health reasons prior to taking learners on a field trip; recording information that a learner is pregnant; as part of pastoral duties); political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the learner's consent. If staff need to record this information, they should use the standard learner information form.

3. 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 college's policy.

4. The college will designate staff in each area as 'authorised staff'. These staff are the only staff authorised to hold or process data that is;

- Not standard data; or
- Sensitive data. The only exception to this will be if a non-authorised staff member is satisfied that the processing of the data is necessary:
- In the best interests of the learner 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 happen only in very limited

circumstances (such as where a learner is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the learner is pregnant or is a Jehovah's Witness).

5. All staff will be responsible for ensuring that all data is kept securely.

6. Staff must not disclose personal data to any learner, unless for normal academic or pastoral purposes, without authorisation or agreement from the designated data controller, or in line with the college's policy.

7. 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 college's policy.

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

Staff Checklist for recording data

• Do you really need to record the information?

• Is the information 'standard' or is it '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 learner or the staff member to collect and retain the data?

• Have you reported the fact of data collection to the authorised person within the required time?