GRIMSBY INSTITUTE GROUP

Data Protection Policy

Grimsby Institute

University Centre Grimsby

Yorkshire Coast College Scarborough

The Academy Grimsby
YOUR FUTURE, FOCUSED

Lincolnshire Regional College

LRAC Lincolnshire Rural Activities Centre

Change Control

Version:	V1.1
New or Replacement:	Replacement
Approved by:	Senior Management Team
Date approved:	01 July 2014
Name of author:	Vice Principal Corporate Services
Name of responsible committee:	Senior Management Team
Name of Corporation committee:	N/A
Date issued:	August 2014
Review date:	June 2017
Document Reference:	GIG-Pol-CS-DataP01

Revision History

Version	Type	Date	History
V1.0	New	18 July 2013	New
V1.1	Updated	25 June 2014	

Contents

Introduction

The Grimsby Institute Group (GIG) needs to keep certain information about its employees, students 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 GIG will comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 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 GIG 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 GIG has developed the following Data Protection Policy.

For the purposes of this policy the GIG incorporates the Grimsby Institute of Further and Higher Education, Yorkshire Coast College, Lincolnshire Regional College, Lincolnshire Rural Activities Centre and The Academy Grimsby.

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 Corporation from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

Any member of staff, student or governor, 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. If the matter is not resolved, it should be raised as follows:-

For staff, through the GIG's Staff Grievance Procedure
For students, through the GIG's Student Grievance Procedure.
For Governors, through the Clerk to the Corporation.

The Data Controller and the Designated Data Controllers

The GIG as a body corporate is the data controller under the 1998 Act, and the Corporation is therefore ultimately responsible for implementation. However, the designated data controller will deal with day-to-day matters.

This Institute's designated data controller is the Vice Principal Corporate Services.

Authorised Staff

The GIG 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 authorised staff are Heads of School, Academy Head, Directors, Curriculum Leaders and GIG Managers and Supervisors. 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 student or staff member, or a third person, or the GIG; 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 student is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the student 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, students and other users are entitled to:

- Know what information the GIG 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 GIG is doing to comply with its obligations under the 1998 Act.

The GIG will therefore provide all staff and students and other relevant users with a standard form of notification by making this policy available on the GIG intranet.

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 that they provide to the GIG in connection with their employment is accurate and up to date.
- Informing the GIG promptly of any changes to information already provided (eg: changes of address).
- Checking the information (about information kept and processed about staff) that the GIG sends out from time to time.

- Informing the GIG of any errors or changes. The GIG cannot be held responsible for any errors unless the staff member has informed the GIG of them.

If and when, as part of their responsibilities, staff collect information about other people, (eg: about students' 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 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 it itself kept securely;
- Only kept away from GIG premises with prior written authorisation from an authorised officer and (where it is held on a computer) on GIG equipment.

Authorised Disclosures

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

These circumstances are strictly limited to:

a. Student data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
b. Student data disclosed to parents/carers in respect of their child's health, safety and welfare.
c. Student data disclosed to parents/carers in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.
d. Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.

Student Obligations

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

Students who use the GIG computer facilities may, from time to time, process personal data. If they do, they must first notify the designated data controller.

Rights to Access Information

In accordance with the law staff, students and other users of the GIG 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.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing.

The GIG reserves the right to make a charge on each occasion that access is requested where significant administrative and/or management time will be involved in meeting the request. The level of this charge will be reviewed by the GIG from time to time and changed as appropriate.

The GIG 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 Students

Requests from students aged 14-16 will be processed as any subject access request and the copy will be given directly to the student, unless it is clear that the student does not understand the nature of the request.

Requests from students 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 child will be processed as requests made on behalf of the data subject (the child) 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 child who is over the age of 16, permission will be sought from the student concerned and data will be sent in a sealed envelope to the requesting parent/carer only if such permission is granted.

Publication of GIG Information

It is the GIG's policy to make as much information public as possible. The GIG has lodged its registration details with the Information Commissioner.

Subject Consent

In many cases, under the Data Protection Act, the GIG can process personal data only with the consent of the individual. In some cases, if the data is sensitive (eg: race or ethnic origin, physical or mental health), **express consent** must be obtained. Agreement to the GIG 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. 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 14 and 18. The GIG has a duty under the Children Act and other enactments

to ensure that staff are suitable for the job, and students for the courses offered. The GIG also has a duty of care to all staff and students and must therefore make sure that employees and those who use the GIG facilities do not pose a threat or danger to other users.

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

Therefore, all prospective staff and students will be asked to sign their Consent to Process which is on the employee application form and the student enrolment card, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn. A separate consent form will be available for parents/carers of the 14-16 Academy students.

In the event that a student withholds consent from the disclosure of any sensitive data (eg: not informing a tutor of their learning difficulty or disability), the GIG will respect that wish, even though it might be seen as disadvantaging their learning.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details, (health and criminal conviction information for 14-16 year olds, will be process inline with legislation). This may be to ensure the GIG is a safe place for everyone, or to operate other GIG 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 students will be asked to give express consent for the GIG to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the designated data controller, Heads of School, Academy Head, Directors, Managers, the Personnel Department or MIS.

Examination Marks

Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide.

Retention of Data

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

- Names and address
- 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 GIG. 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. A list of information with retention times is set out below:-

Data Subject	Data	Period of Retention
Student	Names and addresses Academic achievements Copies of references written	6 years + current year
Student	Any computerised records	Minimum 7 years
Student	Any financial record	6 years + current year
Student	Any health & safety record	40 years
Student	Any accident report	3 years
Student	Other student records	3 years
Staff	Staff records	7 years
Staff	Any financial record	7 years
Staff	Any health & safety record	40 years
Staff	Any accident report	3 years

It is the duty the of the designated data controller to ensure that obsolete data is properly erased.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the Institute. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to Institute 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 Corporation after consultation with staff.

This policy should be read in conjunction with the following:

Safeguarding Policy
Medical Treatment of Students

APPENDIX 1

Staff Guidelines for Data Protection

1. Staff will process data about students on a regular basis, when marking registers, or Institute work, writing reports or references, or as part of a pastoral or academic supervisory role. The Institute will ensure through registration procedures that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the 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.

2. Information about a student's physical or mental health (eg: 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); political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the student's consent. If staff need to record this information, they should use the standard Institute form.

3. All staff have a duty to make sure that they comply with the data protection principles, which are set out in the Institute'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 Institute's policy.

4. The Institute 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 student or staff member, or a third person, or the Institute; 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 student is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the student 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 student, unless for normal academic or pastoral purposes, without authorisation or agreement from the designated data controller, or in line with the Institute'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 Institute'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 student 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?***