THOMAS ROTHERHAM COLLEGE
A tradition of achievement - *A future of opportunity*

Title: Information Security and Data Protection Policy

Author: Chris Walls

Policy Date: September 2016

Review Date: September 2018

Contents:

Cross reference to: Examinations Policy

Publication:

Staff area of Intranet ☑

Student and Public area of Intranet ☑

THOMAS ROTHERHAM COLLEGE
A tradition of achievement - *A future of opportunity*

1. Information Security

Introduction

This information security policy shall apply to information, systems, networks, applications, locations and staff of Thomas Rotherham College.

The purpose of this policy is to enable and maintain effective security and confidentiality of information, both electronic and paper based, processed or stored by TRC. This shall be achieved by:

- Ensuring that all members of TRC staff are aware of and shall comply with relevant legislation, including the Data Protection Act (1998) and the Data Protection (Processing of Sensitive Personal Data) Order 2000.
- Describing the principles of information security management and describing how they shall be implemented within TRC.
- Assisting staff to identify and implement information security as an integral part of their day to day role within College.
- Safeguarding information relating to staff and students under the control of the College

Objectives

Key objectives of this Information Security Policy are to preserve:

- **Confidentiality** - Access to information shall be restricted to those staff and students of TRC and relevant others with agreed authority to view it.
- **Integrity** – Records are to be complete and accurate with all filing and management systems operating correctly.
- **Availability** - Information shall be readily available and delivered to the authorised recipients when it is needed.

Responsibilities for Information Security

- Responsibility for information security shall rest with the Principal. However, on a day-to-day basis the Assistant Principal [Curriculum and Systems] shall be responsible for organising, implementing and managing this policy and its related good working practices.
- The Assistant Principal - Systems shall be responsible for ensuring that both permanent and temporary staff including any contractors [where appropriate] are aware of:-
  - The Information Security policy
  - The Data Protection Principles
  - The ICLT Usage Agreement - outlining personal responsibilities for information security
  - Who to ask or approach for further advice on information security matters.
- All staff shall abide by security procedures of TRC. This shall include the maintenance of College records whilst ensuring that their confidentiality and integrity are not breached. Failure to do so may result in disciplinary action.
- TRC staff shall be responsible for both the security of their immediate working environments and for security of information systems they use, including electronic and paper based systems [e.g. workstations, laptops, Mark books etc.].
- Any contracts with third party organisations that allow access to the information systems of TRC shall be in place before access is allowed. These contracts shall ensure that the staff or sub-contractors of those external organisations shall comply with all the appropriate security policies / guidance required by the College

Thomas Rotherham College shall undertake to ensure:

Contracts of Employment – address information security requirements at the recruitment stage and that all contracts of employment shall contain a confidentiality clause. The information security requirements shall be included within job descriptions.

Access Controls - to areas containing information systems are restricted and controlled to ensure that only authorised staff can access information.

Equipment Security – is effective in order to minimise losses, or damage to the College. All information assets and equipment shall, where possible be physically protected from security threats and environmental hazards. (Locked cabinets (fire proof if possible), and the limitation of risks in the surrounding work area etc.).

Information Risk Assessment –potential risks to the security of College information will be undertaken. Where risks are identified, these should be noted and where possible mitigating action taken.

Security Incidents and weaknesses - are to be recorded and reported to the Assistant Principal [Curriculum and Systems] so that they can be investigated to establish their cause, impact and the effect on the College and its staff and students. (NB. remedial changes arising may need to be included within future staff working procedures, updates to policies and contracts of employment).

Protection from Malicious Software – should be provided through the use of commercial strength anti-virus/anti-malware software. Where there is an internet connection an appropriate firewall shall be installed and managed. No new software shall be downloaded or installed on computer systems of the College without the explicit permission of the IT Manager. Breach of this requirement may be subject to disciplinary action.

Secure Communications – should be in place to ensure that all correspondence, faxes, email, telephone messages and transfer of staff and student records are conducted in a secure and confidential manner.

Business Continuity and Disaster Recovery Plans – are in place so that in the event of a disruption to the information services of the College, it is possible to activate relevant business contingency plans until affected services are restored.

2. Data Protection

Introduction

TRC needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. 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, TRC must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). 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 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

TRC 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, TRC has developed the 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 TRC from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with one of the designated data controllers initially (RWILL/CWALL/SBRID). If the matter is not resolved it should be raised as a formal grievance.

Notification of Data Held and Processed

All staff, students other users are entitled to:

- Know what information TRC holds and processes about them and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what TRC is doing to comply with its obligations under the 1998 Act

TRC will therefore provide all staff and students and other relevant users with a notification of location of personal data and the person to contact for further information. This will state all the types of data TRC holds and processes about them and the reasons for which it is held.

Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to TRC in connection with their employment is accurate and up to date

- Informing TRC of any changes to information, which they have provided, i.e. changes of address
- Checking the information that TRC will send out from time to time, giving details of information kept and processed about staff
- Informing TRC of any errors or changes. TRC cannot be held responsible for any errors unless the staff member has informed TRC of them

If and when, as part of their responsibilities, staff collect information about other people (i.e. about students course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff. (APP 1)

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

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal Information should be:

- kept in a secure office; or
- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, be password protected; or
- kept only on electronic devices which is kept securely

Student Obligations

Students must ensure that all personal data provided to TRC is accurate and up to date. They must ensure that changes of address, etc are notified to the Student Services Administration Manager.

Rights to Access Information

Staff, students and others users of TRC have the right to access any personal data that is being kept about them either on computer or in files (see checklist). Any person who wishes to exercise this right should request and complete the college "Access to Information" form and give it to one of the data controllers.

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 using the standard form.

TRC will make a charge of £50 on each occasion that access is requested although TRC have discretion to waive this.

TRC aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 20 working days 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.

Publication of TRC Information

Information that is already in the public domain is exempt from the 1998 Act. It is TRC's policy to make as much information public as possible. The TRC internal phone list will not be a public document.
Any individual who wishes to make contact with a member of the Corporation should contact the Clerk at the College address in the first instance.

Subject Consent

In many cases, TRC 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 TRC 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 16 and 18. TRC 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. TRC also has a duty of care to all staff and students and must therefore make sure that employees and those who use TRC facilities do not pose a threat or danger to other users.

TRC 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. TRC 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 Consent to Process form, 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.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and family details. This may be to ensure TRC is a safe place for everyone or to operate other TRC policies, such as the sick pay policy or Safeguarding 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 to this prior to any disclosure. More information about this is available from the Data Controllers or H R Department.

The Data Controller and the Designated Data Controller/s

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

TRC has 3 designated data controllers. They are:

Dr Richard Williams	-	Principal
Dr Chris Walls	-	Assistant Principal [Curriculum and Systems]
Mrs Sue Bridges	-	CIS & Exams Manager

Examination Marks [See Examinations Policy]

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

TRC will keep some forms of information for longer than others. Because of storage problems, information about staff and students cannot be keep indefinitely, unless there are specific requests to do so. In general information about students will be kept for a maximum of five years after they leave TRC. This will include in particular:

- name and address
- academic achievements, including marks for coursework and
- copies of any reference written

TRC will need to keep information about staff for longer periods of time. In general, all information will be kept for seven years after a member of staff leaves TRC. 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.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of TRC. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to TRC 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 Principal.

Appendix 1

Staff Guidelines for Data Protection

1. All staff will process data about students 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 students give their consent to this sort of processing, and are notified of the categories of processing, as required by 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; sexual life; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the students consent. If staff need to record this information, they should use the College Information System or contact Student Services.

   E.g.: 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.

3. 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

4. The College will designate staff 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 students 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. A student is injured and unconscious, but in need of medical attention and a member of staff tells the hospital that the student is pregnant or a Jehovah's Witness.
5. Authorised 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 data controller, or in line with the College 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 the College policy.
8. Before processing any personal data, all staff should consider the 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 student 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?

Appendix 2

Standard Request Form for Access to Data

…….. (Name) wish to have access to either

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

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

    - Academic marks of 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)

I understand that I will have to pay a fee of £50

Signed _____

Dated _____

Revised by: CWALL	Date: September 16	Revision No8