TRINITY COLLEGE DUBLIN

ARTHUR COX

Data Protection: A General Overview for Trinity College Dublin[1]

1. Introduction

1.1 Trinity College Dublin collects and uses personal data for a variety of purposes related to its core functions. In doing so, it must comply with national and European legislation which seeks to safeguard the privacy of individuals. This guide seeks to help staff dealing with personal data to do so in a way that complies with the College's legal obligations while upholding the personal rights of individual data subjects. The Information Compliance Office, which sits within the College Secretary's Office, is the primary office responsible for compliance with Data Protection Law within the College.

1.2 The purpose of this guide is to provide staff across the College with a basic understanding of data protection laws as they apply to the College and its principal activities. This guide is not intended to provide specific advice for any particular circumstances so you should consult with the College's Information Compliance Officer if you require specific advice. The current Information Compliance Officer is Sinead MacBride, College Solicitor. Further contact information may be found at http://www.tcd.ie/info_compliance/dp/contact.php

1.3 This guidance note is intended to supplement the College's Data Protection Policy which is available at www.tcd.ie/about/policies/data_protection.php.

2. What is the applicable law?

2.1 The primary legislation governing data protection in Ireland is the Data Protection Acts 1988 and 2003 (the "**DPA**").

2.2 The DPA was enacted in 1988 and amended in 2003 to bring Ireland's law fully in line with the Data Protection Directive (95/46/EC), the European legislation that governs this area of law.

2.3 There is a layer of additional legislation which impinges upon specific areas of data protection, particularly with regard to the issue of direct marketing, which is not covered in this guide. This secondary legislation comprises several statutory instruments including, most notably, the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011. Those parts of the College that engage in direct marketing communications (e.g. the Careers Office) should be aware that specific consent requirements are laid down in these Regulations governing the type of consents (e.g. opt-in or opt-out) that are required before direct marketing contact can be made by phone, email or SMS message.

2.4 The Irish courts have also held that a right to privacy exists under the Irish Constitution, while pursuant to Article 8 of the European Convention on Human

[1] This guide has been prepared by Arthur Cox in association with the College's Information Compliance Officer, Sinead MacBride.

Rights, each individual has a right to respect for his "*private and family life, his home and his correspondence*", subject to certain restrictions that are "*in accordance with law*" and "*necessary in a democratic society*" (which principle was formally transposed into primary Irish law in 2003 through the European Convention on Human Rights Act 2003).

3. Who is the regulator?

3.1 The DPA is enforced and administered by the Irish Data Protection Commissioner (the "**Commissioner**").

3.2 The Commissioner is responsible for upholding the rights of individuals as set out in the DPA, and enforcing the obligations upon data controllers and data processors. The Commissioner is appointed by the government and is independent in the exercise of his functions. Individuals who feel their rights are being infringed can complain to the Commissioner, whose staff will investigate the matter and take whatever steps may be necessary to resolve the matter.

3.3 A useful reference point is the Commissioner's website at www.dataprivacy.ie.

4. When and to whom does the law apply?

4.1 There are a number of key concepts that are critical to an understanding of the law in this area. The main rules are set out in a number of data protection principles which are set out in detail in the DPA. These principles apply to "**data controllers**", "**data processors**" and "**data subjects**". These terms are defined as follows:

(a) A "*data controller*" is a party who either alone or with others controls the contents and use of personal data. For example, the College is a data controller in relation to staff and student data, therefore all College staff are responsible for the safekeeping of data;

(b) A "*data processor*" is as a party who processes personal data on behalf of a data controller. For example, if the College appointed a third party to operate its payroll or if the College outsourced the hosting of its student registration website, the contractors concerned would be "data processors" as they would be processing personal data on behalf of the College (the data controller); and

(c) A "*data subject*" is an individual who is the subject of the processed personal data. Typically within the College we would process personal data relating to students, alumni, staff, visitors to the College etc.

4.2 The DPA applies to data controllers established in Ireland that collect, store or process data about living people on any type of computer or in a structured filing system. While the College as a whole is a data controller, the principles in the DPA governs all of the various units in the college who control the use of personal data.

4.3 The nationality of a data subject does not determine if the DPA applies to the processing of their personal data.

4.4 The DPA does not apply to data kept by an individual for his personal, family or household affairs, or for recreational purposes only.

5. What types of data are personal data?

5.1 "**Personal data**" means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. Common examples of personal data processed by the College include names, addresses, student numbers, photographs, staff numbers, mobile telephone numbers, dates of birth, etc.

5.2 While the Commissioner adopts a broad view of what constitutes personal data, UK case law has provided a narrower definition of personal data (although this interpretation has been criticised by the European Commission and resisted by the Commissioner).

5.3 Factors to consider in determining if data is personal data include:

(a) Is the data about the individual data subject?

(b) Is the data subject the main or primary focus of the data?

(c) Where does the data fall in a continuum of relevance or proximity to the data subject?

(d) Is the data different in some respect because of the data subject's involvement?

5.4 In cases of doubt as to whether data is personal data, please contact the Information Compliance Officer.

5.5 **Sensitive Personal Data**: The DPA provides additional safeguards (and therefore a higher compliance burden for data controllers and data processors) in respect of the processing of "sensitive personal data". "Sensitive personal data" is a subset of personal data, being data relating to racial or ethnic origin, political opinions, religions or philosophical beliefs, trade union membership, physical or mental health, sexual life, and the commission of offences or criminal convictions or proceedings. The enhanced data protection standards which apply to sensitive personal data are set out in Section 2B of the DPA (see paragraph 10.3 below) and these are particularly relevant to the College Health Service, Counselling Service, Disability Service, certain data held by Tutors or other parts of the College who may receive health or conviction data in the course of performing their functions.

6. Is paper/manual data covered?

6.1 The DPA applies to data held in computerised form or in paper form if it is part of a manual filing system. For the purpose of the DPA "*manual data*" means information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system. A "*relevant filing system*" means any set of information relating to individuals to the extent that, although the information is not processed by means of computer, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. The practical result is that structured paper files are covered by the DPA.

6.2 In contrast, "*automated data*" is data that is either being processed by means of equipment operating automatically in response to instructions given for that purpose or recorded with the intention that it should be processed by means of equipment operating automatically.

7. Is all use of data considered to be processing?

7.1 The DPA only applies to the "*processing*" of "*personal data*". However, processing is extremely widely defined to the point that it is difficult to imagine any use of personal data which would not amount to processing for the purposes of the DPA. Hence processing effectively covers all forms of data use (whether active or passive).

8. What are the basic rules?

8.1 Section 2 of the DPA lays down the main data protection principles which govern all processing of personal data by a data controller. These rules can be summarised as follows:

(a) personal data must be obtained and processed fairly;

(b) personal data must be kept for only one or more specified, explicit and lawful purposes;

(c) personal data may not be used or disclosed in any manner incompatible with these purposes;

(d) personal data must be kept safe and secure;

(e) personal data must be accurate and where necessary kept up-to-date;

(f) personal data must be adequate, relevant and not excessive in relation to the purposes;

(g) personal data must not be retained for longer than is necessary for the purposes; and

(h) a copy of the personal data relating to an individual must be given to that individual on written request (subject to certain limited exceptions).

8.2 All data controllers (whether or not required to register with the Commissioner) are required to observe the above data protection principles. Data processors are required to comply with the security principle ((d) above).

8.3 Sections 2A to 2D of the DPA elaborate on the above principles by setting down more detailed requirements regarding consent, notice/transparency, security standards, etc. to be adhered to in order to render processing of personal data compliant with the DPA.

8.4 In addition, Section 8 of the DPA exempts certain narrow categories of processing from the restrictions that would otherwise apply, e.g. processing required to investigate offences, urgent processing required to prevent injury or damage to property, processing required by rule of law, etc. Where those exceptions apply, the College is permitted to process personal data without necessarily addressing the data

protection rules that would normally apply e.g. informing the data subject about the proposed use of the data or seeking consent from the data subject.

9. When is processing considered "fair"?

9.1 **Fair Obtaining**: The most important of the data protection rules is that personal data must be obtained and processed "*fairly*". While the Commissioner has repeatedly stated that this rule requires transparency and full disclosures of all proposed uses of the information at the point of data capture, he does accept that certain obvious uses may be implied by the particular circumstances of the data capture.

9.2 In order for a data controller to obtain personal data fairly, the DPA requires that the data subject (i.e. each individual the subject of the information) "*is provided with, or has made readily available to him or her*" at the time of processing the data, at least the following information:

(a) the identity of the data controller (although this will often be implied);

(b) the purpose behind the data collection;

(c) the persons or categories of persons to whom the data may be disclosed;

(d) any other information which is necessary having regard to the specific circumstances, such as the recipients of the data and the fact that data subjects have a right to access their data (see paragraph 14 below); and

(e) the categories of data concerned, (i.e. name, address, e-mail address, telephone number, etc.).

If the above information is not made clearly available to a data subject, any personal data collected from him or her will not have been collected fairly and the data controller will have infringed Section 2 of the DPA.

For the above reasons it is very important that the College identifies all points of data capture where we seek personal data so as to ensure that appropriate privacy notices, consents etc are obtained and recorded. For example, student registration forms, website forms, booking forms etc should all clearly explain for what purposes the data will be used, to whom it will be disclosed and, if secondary uses are anticipated, such as use for marketing contact, specific consents may be necessary (e.g. through the use of "opt out" or "opt in" boxes).

9.3 **Fair Processing**: In addition to obtaining data fairly, the other core data protection principle is that any processing of data be fair. Usually this requires that consent is in place for the particular use of the data or that the processing is otherwise required in order to fulfil a College obligation (see paragraph 10.2 below). Examples of unfair processing might include:

(a) Emailing a student class list to a researcher to assist in a research project on student behaviours (although note that if the list is fully "anonymised" then the DPA will not apply to it as it is no longer personal data);

(b) Selling a list of alumni to a recruitment company without the consent of the graduates concerned;

(c) Disclosing a student's examination results to a person not specifically authorised by the student to receive them.

10. **Can the College rely on an individual's consent? Is there any other basis for processing?**

10.1 As a general rule, where consent to processing has been obtained from the data subject, processing of the relevant personal data will be permissible.

10.2 Pursuant to Section 2A of the DPA, consent is not necessarily required where the processing is necessary for certain purposes, including:

(a) for the performance of a contract to which the data subject is a party;

(b) for compliance with a legal obligation imposed on the data controller by contract;

(c) where the processing is necessary for a public purpose and for other functions of a public nature performed in the public interest; and

(d) for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed except where the processing is unwarranted by reason of prejudice to the fundamental rights of the data subject.

If the above criteria do not apply, then consent will usually be necessary.

10.3 If processing sensitive personal data, consent cannot be implied and must be "*explicitly given*". In the absence of explicit consent, other pre-conditions for the lawful processing of sensitive personal data (which are set out in Section 2B of the DPA) include where the processing is necessary for:

(a) compliance with employment law obligations;

(b) protecting the vital interests of the data subject;

(c) processing by a not-for-profit organisation (political, philosophical, religious or trade union purposes only);

(d) the obtaining of legal advice and establishing or defending of legal rights;

(e) public functions (administration of justice, etc.); or

(f) medical purposes.

10.4 Given its sensitivity, access to sensitive personal data should be restricted to those members of staff that specifically require such access to carry out their functions and who have received appropriate training in data protection practice and record handling.

10.5 The DPA does not provide any specific minimum age for giving consent to data processing. However, data controllers must decide if a minor (anyone under the age of 18) is capable of appreciating the implications of giving consent. If a person is not able to appreciate the nature and effect of consent (due to physical or mental disability or age), consent should be given on his behalf by a parent, guardian or

relative. The College generally considers all students to be capable of appreciating the implications of giving consent.

11. **Can the College share personal data with third parties?**

11.1 Just like any other type of processing, the disclosure of personal data outside of the organisation must be legitimised by one of the processing justifications under Section 2A of the DPA, as listed above (and, if the disclosed data is sensitive personal data, one of the additional Section 2B justifications listed above).

11.2 The DPA will not prevent disclosure of information where the organisation is legally obliged to make the disclosure (e.g. staff salary details must be provided to the Revenue Commissioners).

11.3 If a disclosure is to be made to a location outside the European Economic Area, one of a specific set of conditions must be satisfied – see paragraph 17 below.

11.4 Sometimes the College enters into contracts that require the transfer of student data, e.g. exchange agreements. These contracts are managed by the Secretary's Office and will contain specific provisions governing the sharing of personal data.

11.5 It is important to exercise caution when disclosing personal data, notably if the disclosure is in response to a request from a third party. For example, rarely, if ever, should information on individuals be given orally to a third party in response to an initial request made over the telephone. Instead, the requesting person or organisation should be asked to make their request in writing. The identity of the requesting individual should be checked in appropriate circumstances.

11.6 In normal circumstances, the College will not disclose personal data to the parents, guardians or other representatives of a student without the student's consent. However, there may be exceptional circumstances, for example, in the case of potential danger to the health or well-being of a student or if a representative such as a solicitor or politician has written to the College making it clear that they are acting on behalf of the student.

12. **What are the security obligations of the College under the DPA?**

12.1 Section 2C of the DPA requires that "*appropriate security measures shall be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data*".

12.2 In determining what an appropriate security measure is, the data controller must:

(a) take into account technological development and the cost of implementing the measures; and

(b) ensure that the measures: provide a level of security appropriate to the harm that might result from any unauthorised or unlawful processing, accidental or unlawful destruction or loss of data; and are appropriate to the nature of the data concerned.

12.3 Appropriate technical security arrangements depend on the nature of the data being processed and the context of the processing, but often include password protection,

data encryption, virus prevention, firewalls, lockable and fireproof filing cabinets, etc. Other measures include the need to train staff in both data protection law and data handling policies. In particular, security issues should be carefully considered when personal data are being destroyed or being transferred outside of an organisation (notably if over a network).

12.4 Further guidance can be found in the extensive IT security policies of the College (http://www.tcd.ie/ITSecurity/policies/) or by contacting the IT Security Officer (in relation to IT security) or College Security (in relation to physical security concerns).

13. How does the College engage third party service providers to process personal data?

13.1 Where the College engages a third party to process personal data on its behalf, it is a legal requirement that the College has in place a contract in writing, which at a minimum, requires the data processor to process the data securely and only in accordance with the instructions of the College. In particular the College must ensure that:

(a) the processing by the data processor is undertaken only in accordance with the College's instructions;

(b) the processing by the data processor is undertaken only for the purposes, and in the manner, stated in the agreement;

(c) its staff are adequately trained in data security measures;

(d) there is a contractual obligation on the data processor to implement and maintain specific security measures, both in terms of physical security and technological security;

(e) the College has rights of access to and inspection of the processor's premises and systems to ensure security measures are being implemented; and

(f) it can control the data processor's ability to sub-contract any of its obligations to third parties.

Agreements to engage third party service providers to process personal data are managed by the Secretary's Office.

14. Can individuals seek access to their personal data?

14.1 Data subjects have certain rights conferred under the DPA, the most significant right being perhaps the right to obtain a copy their personal data.

14.2 Within 40 days of a data subject access request (subject to the data subject paying a maximum fee of €6.35), a data controller must:

(a) confirm whether the data kept includes data relating to the data subject;

(b) supply the data subject with a copy of such data in intelligible form (subject to a "*disproportionate effort*" exemption);

(c) inform the data subject of the purpose(s) for the processing of his/her data;

(d) notify the data subject of the identity of those to whom the data controller discloses the data;

(e) inform the data subject of the source of the data, unless it is contrary to public interest; and

(f) explain the logic involved in automated decisions.

14.3 The right of access is extremely wide-ranging. Unless a relevant exemption applies (see below), an individual is generally entitled to see their personal data contained in all locations.

14.4 It should be noted that an individual is entitled to see only his/her own personal data, not any information which relates to anyone else or more general records (although in some cases that information may be available under the College's Freedom of Information procedures).

14.5 There are very limited grounds for refusing a data subject access request and there is no carve out for defamatory statements, harmful content or commercially sensitive information. Furthermore the Commissioner tends to the view that a broad interpretation of personal data should apply in relation to managing access requests.

14.6 An individual's request for health data may be refused if disclosure of the information is likely to seriously damage the physical or mental health of the data subject (Data Protection (Access Modification) (Health) Regulations, 1989 (S.I. No. 82 of 1989)). Data controllers or data processors (if they are not health professionals) must consult with the individual's doctor before disclosing health data. Similar exemptions are available in respect of access to social work data (under the Data Protection (Access Modification) (Social Work) Regulations, 1989 (S.I. No. 83 of 1989)). Disclosure of this data can be refused if it is likely to cause serious damage to the physical or mental health or emotional condition of the data subject. This may be a specific concern in the case of data processed by the College or service providers in the context of student or staff counselling services.

14.7 A highly significant decision of the English Court of Appeal, Durant v Financial Services Authority in 2004, dramatically restricted the scope of data protection legislation in England and Wales and specifically the scope of access requests. The Court held that to be part of a data subject access request the data must "*relate to*" the individual in some meaningful way. Two relevant considerations highlighted by the Court were whether the information was biographical in a significant sense and whether the information focused on the individual.

14.8 To ensure a coordinated and appropriate response to data access requests, all such requests should be directed to the College's Information Compliance Officer.

15. What about Examination Data?

15.1 Examinations data which identifies any particular student is "personal data" and therefore it is subject to the data protection rules detailed above. For this reason, care should be taken to publish examinations data as anonymously as possible (e.g. student numbers instead of names). Further, if an accommodation has been offered to a student who may suffer from a disability, this "sensitive personal data" should not

be shared with any parties within the College unless they have a need to know it so as to ensure the accommodation is provided.

15.2 The right of access to examination data is specifically dealt with in the DPA. The right for students to access their scripts and discuss their performance is outlined in s. 51 of the General Regulations and Information Section of the College Calendar (page H11). Students wishing to access their scripts must do so in accordance with these regulations, and should therefore in the first instance contact the relevant Director of Undergraduate Teaching and Learning or Course Coordinator.

16. What other express rights do data subjects have under the DPA?

16.1 Automated Decisions

A data subject has the right, by notice, to prevent the data controller from taking evaluation decisions that would '*significantly affect'* him or her, by automated means alone. Additionally, where personal data are being processed automatically for the purpose of evaluating matters relating to the data subject and the processing has or is likely to be the sole basis of a decision significantly affecting the data subject, he or she is entitled to be informed by the data controller of the logic (save to the extent that it constitutes a trade secret) behind the decision taking.

16.2 Right of rectification and erasure

Data subjects have a right to have data that is held in contravention of the data protection principles rectified or erased within 40 days of the request being made. Where a data controller complies with such a request he shall, as soon as may be and in any event not more than 40 days after the request has been made, notify the individual making the request, and if such compliance materially modifies the data concerned, also notify any person to whom the data was disclosed during the 12 month period prior to the request being made, unless such notification proves impossible or involves a disproportionate effort.

16.3 Duty of Care

Data controllers and data processors owe a duty of care to the data subject (under Section 7 of the DPA) in relation to the collection of, and dealings with, personal data. Injury suffered by a data subject may include damage to reputation, possible financial loss or mental distress. A data subject can bring a civil action in the Irish courts against the data controller or data processor for a breach of duty of care, although to date such claims have been rare. Note the rights under Section 7 are in addition to the right of the Commissioner to investigate complaints made by data subjects.

17. Do special rules apply if I transfer personal data outside of the EU?

17.1 Section 11 of the DPA prohibits the transfer of personal data to a country outside the European Economic Area ("**EEA**") unless such country ensures an "*adequate level of data protection*".

17.2 Other than with respect to transfers of personal data to certain "**safe countries**" (e.g. Argentina, Canada, Switzerland, Guernsey, The Isle of Man, Jersey, Faroe Islands, etc.) special conditions must be met before transferring personal data outside the

EEA, where the importing country does not have an EU-approved level of data protection law.

17.3 Transfers are ordinarily managed using a combination of data subject consent; European Commission approved '*model form clauses'*, the '*Safe Harbor*' scheme (for data exports to the US); and/or (less frequently) binding corporate rules.

17.4 Cross border transfers of data can also be legitimised where the transfer:

(a) is required by law;

(b) takes place with the data subject's consent to the transfer;

(c) is necessary for the performance of a contract to which the data subject is party;

(d) is necessary for the taking of steps at the request of the data subject with a view to entering a contract with the data controller;

(e) is necessary to conclude or perform a contract between the data controller and someone other than the data subject in cases where the contract is entered into at the request of the data subject or where the contract is in the interests of the data subject;

(f) is necessary for reasons of substantial public interest;

(g) is necessary for obtaining legal advice or for legal proceedings;

(h) is necessary to: prevent injury or other damage to the data subject's health; prevent serious damage to his property; or protect his vital interests in some other way; or

(i) is authorised by the Office of the DPC.

17.5 No units of the College should transfer any data outside the EU without first contacting the Secretary's Office and IS Services. This includes the uploading personal data to a cloud server which is based outside the EU (see further TCD Cloud Computing Policy)

18. What are the powers of the Data Protection Commissioner?

18.1 The Commissioner has the power to:

(a) carry out investigations as he sees fit, in order to ensure compliance with the DPA and to identify possible breaches;

(b) obtain information and issue enforcement notices (in respect of contraventions which are not criminal offences in themselves) requiring the persons or legal entities to take steps that may include ceasing data capture or processing until its data activities comply with the law. Failure to comply with an enforcement or other notice issued by the Commissioner constitutes an offence;

(c) prepare and publish codes of good practice for guidance in applying the law to particular areas. This supplements the Commissioner's existing power to approve codes of practice drawn up by trade associations.

(d) bring prosecutions and ask the courts to impose criminal fines on data controllers / processors or directors, managers or other officers of companies which may be data controllers or data processors, where it can be shown that an offence has been committed with the consent or acquiescence of any such officer or other member. If data controllers or processors or other associated persons are found guilty of an offence under the DPA, they are liable on summary conviction to a fine not exceeding €3,000 and on indictment, to a fine not exceeding €100,000. A court may also order the forfeiture, destruction or erasure of data connected with the offence by an individual so convicted.

18.2 Enforcement action by the Data Protection Commissioner may also lead to negative publicity for the College.

19. **Must I register my processing with the Commissioner's office?**

19.1 While all data controllers must comply with the data protection principles, at present not all data controllers are required to register with the Commissioner's office.

19.2 The following organisations must register:

(a) government bodies / public authorities;

(b) banks and financial / credit institutions;

(c) insurance undertakings (not including brokers);

(d) persons whose business consists wholly or mainly in direct marketing;

(e) persons whose business consists wholly or mainly in providing credit references;

(f) persons whose business consists wholly or mainly in collecting debts;

(g) internet access providers;

(h) telecommunications network or service providers;

(i) anyone processing personal data related to mental or physical health (e.g. health professionals;

(j) anyone processing genetic data; and

(k) anyone whose business consists of processing personal data for supply to others, other than for journalistic, literary or artistic purposes.

19.3 Currently certain parts of the College are registered with the Commissioner, for example, the College's Centre for High Performance Computing and the College's TILDA (Irish Longitudinal Ageing) Study. All registrations and renewals should be coordinated through the College's Information Compliance Officer.

19.4 It is an offence to process personal data without an appropriate entry on the register of data controllers, unless an appropriate exemption exists. Trinity College Dublin is exempt from the requirement to register as an educational establishment that is a university, although this does not affect its requirement to comply with Data Protection Legislation.

20. What rules apply to the retention of personal data?

20.1 It is a requirement of data protection law that personal data is not kept for longer than necessary for the purpose for which it was acquired. No specific retention periods are set by the DPA. Instead, each organisation must consider for how long it will require various types of information and then set specific retention periods (under for instance applicable employment law, tax law, the Statute of Limitations, etc.). Personal data should always be kept at least as long as any relevant statutory limitation period.

20.2 Retention periods may also be influenced by the obligatory retention periods set by external professional regulators.

21. Is it a requirement to nominate a data protection officer?

21.1 No. While not strictly required by the DPA, the College has appointed an Information Compliance Officer who will assist the College and its staff in complying with the data protection legislation.

21.2 It would be useful for each area to nominate a Data Protection Liaison Person to link in with the Information Compliance Officer to assist in managing Data Protection obligations locally.

22. What reforms are proposed to data protection law?

22.1 The European Commission, the European Parliament and the European Council are presently discussing proposals for an overhaul of data protection rules in the European Union. The proposal, if adopted, will increase compliance obligations of data controllers, with the possibility for fines of up to 5% of global turnover being imposed on the offending party. The rationale is to reform the law so that a unified data protection regime will exist across the EU. It is expected that the new law will be enacted by Regulation and that the changes will be in force in the coming years (although this is subject to revision based upon the progress of the above mentioned discussions).

23. Other Relevant College Documents and Policies

23.1 The College has a range of published policies which are available at **www.tcd.ie/about/policies**. Some of these policies have specific data protection implications. For example:

(a) Data Protection Policy

(b) Child Protection Policy

(c) CCTV Policy

(d) IT and Network Code of Conduct

(e) IT Security Policy

(f) Mental Health Policy

(g) Records Management Policy (which is currently subject to review)

This guidance note should be read in conjunction with the College's Policies and in the event of any conflict, the College's Policies will prevail.

13 June 2014