An Coimisinéir Cosanta Sonraí
Data Protection Commissioner

<u>Institute of Technology, Carlow</u>

Final Report of Inspection Issued August 2013

1. LEGAL BASIS FOR INSPECTION

Section 10(1A) of the Data Protection Acts 1988 & 2003 states that

"The Commissioner may carry out or cause to be carried out such investigations as he or she considers appropriate in order to ensure compliance with the provisions of this Act and to identify any contravention thereof".

Under this authority the Commissioner instructed that an inspection of the Institute of Technology, Carlow (IT Carlow) be conducted. An Inspection Team was selected, consisting of Eunice Delaney, Assistant Commissioner, John Rogers, Senior Compliance Officer and Sinéad McAuley, Compliance Officer.

2. PRE-INSPECTION

A letter (Appendix 1) was sent to IT Carlow by email on 21 February 2013, giving notice of an intention to conduct an inspection on 21 March 2013. The purpose of the Inspection was described as being:

> *To ascertain if the procedures and practices employed by IT Carlow are in compliance with the provisions of the Data Protection Acts, 1988 and 2003*

The letter advised that attention would focus on the following data protection principles:

- Fair obtaining and processing of personal data
- Ensuring data is kept for one or more specified, explicit and lawful purposes
- Disclosure / further processing / transfer of data to a Third Country
- Ensuring the data processed is adequate, relevant and not excessive
- Ensuring the data processed is accurate, complete and up-to-date
- Data Retention: ensuring personal data is kept for no longer than necessary
- Safety & Security of Data
- Access Requests

In advance of the audit, the Office of the Data Protection Commissioner indicated to IT Carlow that the following areas, in particular, would be examined during the course of the inspection:

- Student Admissions & Student Registrations
- HEA Access Survey
- Access Office
- Data Transfers:
  - Data received from CAO
  - Data submitted to HEA
  - Other student data transfers
- Records Management e.g. student records, retention schedules
- Data Protection/FOI Access Requests
- Security

3. THE INSPECTION

3.1 Introduction

The Inspection Team met initially with David Denieffe, Registrar and subsequently with Mary Jordan, Head of Academic Administration and Student Affairs, Helena Johnson, Head of Student Services, Muirghin Brophy, FoI/Data Protection Officer and Fergal Flanagan, Head of Computing Services during the course of the audit.

Overview of IT Carlow

IT Carlow was founded in 1970 and currently caters for approx 3,870 full-time and 1,650 part-time students. IT Carlow has 260 full-time staff with a further 200 part-time workers. The Institute has three campuses, with the main campus located in Carlow town. A second smaller campus is located in Wexford town and a third in Rathnew, Co. Wicklow. IT Carlow indicated to the Team that IT Carlow is one of the largest providers of third level part-time courses in the State. Overall, IT Carlow's research facilities have grown by 30% in the last 5 years with courses offered drawn from Sciences, Engineering, Business & Humanities.

3.2 Obtaining and Processing of Personal Data

The Inspection Team met with Mary Jordan, Head of Academic Administration and Student Affairs, to examine student admissions, student registration and the HEA Access Survey.

Banner is a system widely used across the Institutes of Technology (13) and is in use in IT Carlow since 2003. It was indicated that the majority of students applying for full time courses apply through the CAO (Central Applications Office) route.

IT Carlow outlined that applications made through the CAO are automatically uploaded onto Banner whilst non-CAO applications (part-time/evening courses) are made manually on paper application forms which are then uploaded onto Banner also.

IT Carlow clarified to the Team that the number of points the student has attained in the leaving certificate is provided by the CAO together with the student's leaving certificate results and this data is uploaded onto Banner as part of a candidate's overall application. The Team was informed that 1,200 first year students registered for a course in IT Carlow in September 2012.

IT Carlow clarified that applications may or may not result in actual registrations depending on any subsequent offers made to applicants for places on other courses higher up their list of preferences. IT Carlow stated that in a case where an applicant does not proceed to enrolment stage, his or her record will be purged from Banner in May/June of the following year when preparing for the first data upload for the next Academic year. However, if the applicant does enrol, but subsequently leaves the Institute, his or her record will be retained on the system. IT Carlow indicated that this record may be important in terms of identifying any details of fees paid or with regard to the claiming of free fees. The Team addressed retention with IT Carlow in more detail later in the audit (see section 3.5).

3.2.1 PPSN

When a student is accepted, s/he must register with the Institute and complete an enrolment form (see appendix 2) which is stored on the Banner system. The Team noted that the enrolment form seeks the student's PPSN. IT Carlow stated that it is required by the Higher Education Authority (HEA) to seek the student's PPSN and provide it as part of the Institute's returns to the HEA. IT Carlow also stated to the Team that the PPSNs of all registered students are also supplied to the Department of Social Protection each November in an exercise to enable the Department to check for any instances of social welfare fraud – individuals who are in full–time third level education while at the same time claiming unemployment assistance or benefit. Banner creates an excel report which contains details of every full-time student registered with the Institute. IT Carlow confirmed to the Team that the report is password protected and emailed to the Department of Social Protection.

The legislation governing the allocation and use of the PPS Number is contained in the Social Welfare (Consolidation) Act, as amended by the Social Welfare Acts 1998, 1999, 2000, 2002, 2003 and 2005 and the Social Welfare and Pensions Act 2007. Only Specified Bodies named in the above Social Welfare Acts can use the PPS Number. The Office of the Data Protection Commissioner notes that IT Carlow is a specified body under Social Welfare legislation.

The Team checked IT Carlow's entry on the Register of Users[1] authorised to use the PPSN and noted it stated the following

Institute of Technology Carlow
(i) Does your Institute use the PPS Number at present?

No.

(ii) For what purpose(s)?

Not Available.

(iii) Does your Institute exchange the PPS Number with any external body? If so please name the relevant bodies and state the purpose(s) of the exchange

If available it would be included in reports to the Department of Social and Family Affairs. Revenue Commissioners for tax purposes.

(iv) What future plans has your Institute for the use of the PPS Number?

No plans to the moment.

[1] http://www.welfare.ie/en/Pages/Personal-Public-Service-Number-Register-of-Users.aspx

IT Carlow indicated that it does not itself use the PPSN for any reason, although the Team noted that as well as being sought on the Enrolment Form the PPSN is entered on Banner in its complete form. The Office of the Data Protection Commissioner advises IT Carlow to contact Client Identity Services in the Department of Social Protection with a view to amending its entry on the register of PPSN users in light of its collection of students' PPSNs for the purposes of submitting returns to the Department of Social Protection and the HEA. The ODPC recommends in the first instance that IT Carlow's enrolment form is amended to clearly state the reasons for which the PPSN is being sought (HEA returns and Department of Social Protection anti-fraud checks). In addition, the ODPC does not see any basis for the PPSN to be stored within Banner as part of a student's general record. At a minimum, it is recommended that the PPSN is masked on the system with access to the full PPSN visible only to the staff submitting the returns to the HEA and Department of Social Protection.

[Since the inspection took place, IT Carlow indicated that it will put a mechanism in place which will mask the PPSN in Banner].

3.2.2 Enrolment Form

When examining the Enrolment Form (appendix 2) the Inspection Team noted that wording contained at the foot of the form states that "…the institute may provide data on me to employers or professional bodies and other third parties…" IT Carlow clarified to the Team that other third parties would include the HEA and the Department of Social Protection. IT Carlow indicated that it would not pass on data to employers or professional bodies without the consent of the individual and that often these disclosures would be at the request of the individual themselves.

At registration, a photograph is taken of the student and an id card produced which includes the photo together with the student's name and the name of the course being undertaken. IT Carlow confirmed to the Team that the card does not display date of birth. The photo is electronically held on the student's record within Banner.

The Enrolment Form also states that IT Carlow "…may use my address / photograph in publications of the Institute where they judge this to be in the best interest of myself or the Institute." The Enrolment Form, which must be signed by the student, does not provide any opt-out for the student in terms of having his or her image processed by the Institute. The Team noticed that this clause is contained on a number of other application forms, for example, the Lifelong Learning Application (appendix 3). It is recommended that all forms containing this clause are amended to include a 'tick box' to allow the student to opt out of having his or her image processed in this manner.

3.2.3 Banner

As already mentioned above, Banner is the student record system in operation in IT Carlow. The system not only provides for the management of student records, but also allows the students themselves to access and manage certain personal information within the system. The Inspection Team examined Banner in detail, noting each of the screens available to staff. The system holds student data (including PPSN and photo as outlined above) and course details, dates and amounts of fees paid and exam results. Various screenshots from the system are appended at appendix 4.

In terms of students using Banner, an e-mail address and PIN is generated for every student. Entry of the PIN allows the student to enter the Banner Self Service system where a variety of functions can be performed, for example, amending address details. It is also possible for the student to access year on year exam results through the 'Grademailer' feature within the Banner system. It was indicated to the Team that the information returned through Grademailer does not pull the student PPSN from Banner.

IT Carlow clarified that students who login to 'Web for Students' receive a warning message stating that unauthorised access is forbidden.

3.2.4 European Diploma Supplement

IT Carlow outlined that another portal referred to as Digitary, allows graduate students to access their academic qualifications as detailed on their 'European Diploma Supplement' (see appendix 6). The Team learned that the European Diploma Supplement was developed under a movement referred to as the 'Bologna Process' and was adopted jointly by UNESCO and the Council of Europe. A common national format was devised for the Diploma Supplement in Ireland by the National Qualifications Authority of Ireland (now Quality and Qualifications Ireland/QQI).

The Diploma Supplement provides additional information regarding a student's award which is not available on the official IT Carlow graduation certificate such as the nature of the programme completed by the student, the level of the qualification and the results gained and entry requirements and access opportunities to the next level of education etc. The Team learned that the aim of the Diploma Supplement is to make a graduate's results more easily understood, especially for employers and institutions outside the issuing country.

It was outlined to the Team that a student, via Digitary, can provide prospective employers with access to their Diploma Supplement if they actively choose to do so. The information on the Diploma Supplement is pulled through from Banner. IT Carlow clarified to the Team that the European Diploma Supplement currently produced directly from Banner includes the PPSN number where it is held in Banner. The Team examined a blank hard copy of the European Diploma Supplement (see appendix 6) and noted that section 1.4 of the form was headed '**Student Identification number or code'**.

[Since the audit took place the ODPC raised the export of student PPSNs into the European Diploma Supplement with the Department of Social Protection as it could not see that there was any legal basis for the transfer of this data. The Department of Social Protection responded indicating they had reviewed and subsequently contacted Quality and Qualifications Ireland(QQI) and instructed QQI to cease collecting

PPSNS for this purpose and to issue sectoral guidance to all educational institutions in this regard.]

When logging onto Digitary, the Team noted that a warning is displayed stating that unauthorised access is forbidden and all traffic to this server is logged (see appendix 5).

3.2.5 HEA Access Survey

Since 2007, higher education institutions in receipt of funding from the HEA (including IT Carlow) gather information on students' social, economic and cultural background by means of a survey of first time students at IT Carlow. This information assists the HEA in advising on future funding policy and to monitor evidence of progress with regard to opening up access. Participation in the survey is non-mandatory (see information leaflet at appendix 7). The Team noted that the non-mandatory nature of the survey stems from a complaint investigated by the ODPC in 2006/2007where the requirement to complete the survey was queried. The ODPC upheld the complaint and instructed the HEA to ensure the completion of the survey was voluntary.

As the Access Survey File itself contains fields relating to any physical or learning disabilities, mental/emotional health, ethnic/cultural background, the data is considered to be "sensitive" data within the meaning of the Data Protection Acts 1988 & 2003, with extra safeguards and obligations attached to the processing of this data.

Students in IT Carlow complete the access survey online as part of the registration process (see survey screenshots at appendix 8). The Team noted the first question is as follows

1. Please select 'No' if you do not want to complete these Equal Access questions
    - Yes
    - No

IT Carlow clarified to the Team that 75% of students registering for the first time at IT Carlow completed the survey in 2011/12.

IT Carlow outlined to the Team that a number of steps are then undertaken in providing the survey information to the HEA. In December each year, the raw survey information is extracted from Banner and emailed to a coder working for the HEA who assigns predetermined codes to the data and resubmits the datasets to IT Carlow in January/February. This coded dataset is then uploaded to Banner. Finally, the coded data, together with student data already held on Banner is extracted from Banner in four agreed reports. These four XML files are then uploaded to the HEA in March by the Institute via a specific username and password.

In all, the Team noted that four individual files are uploaded to the HEA: the Access Survey File, Course File, Program File and Survey File (this file contains student enrolment records, including PPSN). The files are in xml format. Included in the four files being returned to the HEA, in addition to the information provided by the student participating in the access survey, are the IT Carlow's unique student id and the student's PPSN where available (although the access survey itself does not seek the PPSN). As mentioned earlier, IT Carlow indicated it was required to provide student PPSNs to the HEA where they have been provided. Having examined the returns being made to the HEA, the Team observed that around 10% of students did not provide their PPSNs. Of concern to the ODPC is the potential ability of the HEA to identify students if it gathers PPSN and student ids (in addition to CAO numbers received from the CAO). The Team noted that the Equal Access Survey leaflet (see appendix 7) states

> "Equal Access information is stored alongside other student data in the HEA (including nationality, age, course details) but no data includes name or addresses."

The Team confirmed that no names or addresses were supplied in the returns it viewed as having been submitted to the HEA by IT Carlow.

The ODPC indicated that it has been developing a broader and more detailed view of data flows within the third level sector generally. This has included engagements with individual educational institutions, the HEA and the CAO. Issues around the collection of a variety of identifiers by the HEA were identified during the course of these engagements. The ODPC wrote to the HEA in April 2010 to outline its view that it "considers that datasets containing CAO numbers and PPSNs do constitute personal data and therefore we await proposals as to how the HEA wish to make this process compliant with the requirements of the Acts". The ODPC has for some time had concerns regarding information flows within the higher education sector which initially may not appear to render students identifiable, but ultimately when connected with other datasets, may allow these individuals to be identified. Previously the HEA indicated to the ODPC that "data is only ever circulated in an aggregated form and that no HEA reports publish data on an individual level". At the time the ODPC recommended that the HEA continue to take adequate steps to ensure that it was not possible to identify individual students from statistical information.

One point of note relating to the upload of information to the HEA observed by the Team was that, in relation to second year students, the survey information which would have been uploaded for those students in year one was subsequently stripped out of the returns submitted to the HEA the following year. As IT Carlow indicated that it does not use or analyse the access survey data in any way, the Inspection Team considered the deletion of this information to be good practice.

3.3 IT Carlow Access Office

The Access Office in IT Carlow coordinates academic supports within the Institute to students with disabilities and students in financial difficulties. Both categories of funding - the Fund for Students with Disabilities (FSD) and the Student Assistance Fund (SAF) - are funded by the Irish Government and part-funded by the European Social Fund under the Human Capital Investment Operational Programme 2007-2013. The Inspection Team met with Helena Johnson, Head of Student Services, to examine how the personal data of students is processed by the Access Office.

It was indicated to the Team that IT Carlow fields applications from students in both categories under the Carlow Access Programme (CAP). The Programme mirrors the DARE (Disability Access Route to Education) and HEAR (Higher Education Access Route) schemes available to applicants to other third level educational facilities.

Under CAP, an application for disability supports may be made under the following headings:

- Specific Learning Difficulties
- Physical Disability
- Blind & Visually impaired
- Deaf & Hard of Hearing
- Mental Health
- Aspergers
- ADHD or ADD
- Significant ongoing illness/other

The following areas are considered when assessing an application for financial supports:

- Long-term unemployment
- Low family income
- Little or no family tradition of progression onto Higher Education
- Under represented socio-economic groups in Higher Education

IT Carlow outlined that an applicant for disability supports may apply to some higher educational institutions as part of their CAO application by providing details of his or her disability. If the applicant is applying specifically to IT Carlow, or is offered a course in IT Carlow, IT Carlow indicated that an individual must complete IT Carlow's CAP Disability Entry Programme Application Form (see appendix 9). This form includes a section seeking the applicant's permission to download his or her disability information from their C.A.O. application which IT Carlow has access to if they have included IT Carlow as one of their choices. IT Carlow clarified to the Team that all registered students seeking supports with their disability register with the Access Office and that all registered students with a disability complete a 'Needs Assessment Form' which remains in the Access Office (see appendix 34). IT Carlow confirmed that registered students do not complete a Fund for Students with Disabilities Form to be returned to the HEA.

All registered applicants with a disability are provided with appropriate supports such as special laptops, special tutoring, or personal assistants. The Team noted that applicants to the Disability Entry Programme are informed that this programme "will consider applicants with a disability for reduced points".

IT Carlow clarified to the Team that declaring a disability and receiving appropriate support does not ever qualify a student for additional marks in terms of examination grades. The Team noted that students who have applied under the scheme are informed in writing that details regarding their "disability will be disclosed discreetly to relevant staff as necessary in order to support you through your course" (see appendix 10). The letter also gives an undertaking that any documents provided by applicants for the programme will be kept confidential. It was indicated to the Team that, in some cases, the Access Office may seek additional medical information if it is unsure as to the precise medical condition of the student. For example, in the case of a student with a mental health condition, the Access Office may need to discuss the condition with the student's doctor or parents with the prior knowledge of the student that this consultation was to be required in order to adequately meet the student's needs. If there is a possibility that a student may be a threat to others, IT Carlow indicated that an external organisation such as An Garda Síochána would be alerted in line with common practice and national guidelines. IT Carlow indicated that such instances are rare and at the same time they would verbally inform the student that they are escalating the information to the relevant organisation.

The Team was informed that lecturers may, from time to time, approach the Access Office in terms of having additional supports made available to a student with a disability. The Medical Officer may similarly approach the Access Office if a particular medical issue is identified which could be supported by the Access Office. It was indicated that, in such situations, the Access Office is not provided with access to the student's medical file and that the Access Office would not ever seek such information in the first instance.

An applicant for financial support must complete the CAP Financial Supports application form (see appendix 11) and if successful in their application, the SAF Funding application form (see appendix 12). In support of an application, the student must provide verification documentation such as P60 and other financial information and documentation to assess the candidates as well as information on the specific types of support being sought.

IT Carlow outlined that it is intended that from September 2013, if the applicant has already applied to the HEAR (Higher Education Access Route) scheme at CAO stage, s/he can indicate their consent to authorise IT Carlow to access this information on their CAO application similar to the authorisation students give to IT Carlow to access information supplied under DARE (Disability Access Route to Education) on the C.A.O. application.

IT Carlow outlined that the application process to receive financial support involves an interview with the IT Carlow Finance Committee which ultimately makes a decision on the application.

Details of the supports provided to students under the Fund for Students with Disabilities (FSD) and the Student Assistance Fund (SAF) are returned to the HEA. The HEA also gets details on the number of recipients in each category. Returns are made quarterly, though it was indicated to the Team that these returns do not contain any student personal data. However, a combined FSD and SAF return is made annually which does contain personal data in the form of the name of the student and student id number. IT Carlow subsequently clarified to the ODPC that for the year 2012, they were not required to submit an annual return to the HEA.

IT Carlow demonstrated to the Team that files on FSD and SAF applicants are held in separate areas of the Student Services Offices in locked cabinets. It was indicated that the Student Services Offices itself is locked when vacated. The Inspection Team examined both areas from a security perspective with no issues arising.

The Inspection Team also examined a number of files in each area. In relation to FSD files, the Team viewed applications, psychological reports and CAO information. In one case, a mental health applicant, the Team noted a psychiatric report on the file. It was indicated that in such a case, details of the health issue would be sent to the head of department responsible for the student who, in turn, would provide relevant information to the course tutors. This process is set out in the Student Disability Policy which is included in the Student Handbook (appendix 13).

3.4 Data Protection/Freedom of Information

Section 2(1)(c) of the Data Protection Acts 1988 and 2003 provides that a data controller shall not retain personal data longer than is necessary for the purpose or purposes it was obtained. In determining appropriate retention periods for personal information, data controllers must have due regard for any statutory obligations. If the purpose for which the information was obtained has ceased and the personal information is no longer required, the data must be deleted or disposed of in a secure manner.

The Inspection Team met with Muirghin Brophy, FoI/Data Protection Officer, to discuss IT Carlow's data retention policy and data protection/freedom of information access requests. With regard to access requests, it was explained that IT Carlow has never received a request for personal data under the Data Protection Acts but that, should one be received, it would be directed centrally to the FoI/Data Protection Officer.

It was also indicated that the IT Carlow FoI/Data Protection Officer is involved in a group made up of FoI Officers from each of the 13 Institutes of Technology which is actively examining a common retention policy. The group meets quarterly and has devised a draft discussion document.

The Team indicated to the FoI/Data Protection Officer that a Department of Finance FOI Central Policy Unit's Notice No. 23[2] offers guidance to public bodies on how to harmonise their approaches to granting access whether the request is made under the Freedom of Information or Data Protection Acts.

3.5 Retention of Personal Data

Prior to the audit, IT Carlow supplied the Team with a records retention schedule (appendix 14) which detailed the types of records held by IT Carlow and the retention requirements for each one.

[2] http://www.dataprotection.ie/docs/Important-new-data-protection-guidance-for-all-public-sector-bodies/411.htm

Where an applicant actually completes the registration process, IT Carlow confirmed that it retains their Student Record on Banner indefinitely. The ODPC considers that a facility should be devised to allow for the archiving of student stored on the Banner system after a defined period of time. The Team also noted that IT Carlow's retention policy (see appendix 14) outlines initially that student records are retained permanently 'if there is a business reason to do so'. However the retention schedule proceeds to state that student personnel files are deleted one year after a course has been completed and attendance registers are scheduled to be retained for 7 years only. In addition to these core student records, the ODPC notes that IT Carlow's retention schedule states that examination papers and results – broadsheets are retained permanently but there is a distinction drawn in the schedule with regard to examination scripts, solutions and continuous assessments all of which are retained for 18 months.

The Inspection Team commended IT Carlow on the comprehensive content of the retention schedule.

In general, across the higher education sector the ODPC recommends that a critical analysis is conducted of what portion of a student's record needs to be maintained after they leave university.

The Team noted that the student's leaving certificate results are also retained permanently as part of the student record. The issue regarding the necessity (or not) for third level institutions to retain records of an individual's leaving certificate results and CAO choices is of interest to the Office of the Data Protection Commissioner. In 2007, the Office dealt with a complaint received by a graduate of a third level institution who made a subject access request and subsequently objected to his leaving certificate results and CAO choices still being in the possession of that third level institution. At the time, the institution argued that the capture and retention of an individual's leaving certificate results stemmed from the leaving certificate exam replacing the traditional matriculation exam, and that the university in question used the leaving certificate results as evidence of the student having been 'matriculated'. The matter was resolved when the educational institution agreed to delete the data subject's records. The ODPC considers that the retention of leaving certificate results – being equivalent to the old matriculation examination - may be justified but does not consider there is any good reason to retain CAO preferences permanently. The wider implications of such a policy being prevalent throughout the third level sector will be addressed by the Office of the Data Protection Commissioner going forward with the sector as a whole.

In the meantime, this Office advocates the use of anonymised data to conduct any research in IT Carlow regarding leaving certificate results, entry standards and college retention rates.

3.6 Disclosure of Personal Data

Bulk disclosures of personal data from IT Carlow to the HEA and from the CAO to IT Carlow have been examined earlier in this report.

IT Carlow indicated that An Garda Síochána makes only a handful of requests for student data each year. Requests are made in writing, though on occasion requests may be by telephone. The Inspection Team recommended that all such requests be followed up in writing on garda headed paper and that a log of such requests is kept. IT Carlow outlined that there is a Garda Liaison Officer attached to IT Carlow and that regular meetings take place between AGS and IT Carlow. In terms of students who have received ASBOs, IT Carlow stated that it is the students who clarify to IT Carlow if they have received ASBOs. The ODPC advises IT Carlow that the disclosure of information regarding a student's ASBO should not occur or be recorded by any third party in the absence of there being any legal basis to do so. Section 8 of the Data Protection Acts should be examined in this regard.

IT Carlow also stated on the day that the Student Services Office would call in a student if it received a complaint from a local resident regarding student behaviour.

3.7 IT Carlow Website

On 1 July 2011, Statutory Instrument No. 336 of 2011 (SI 336 of 2011) came into law in Ireland. This instrument introduced a number of amendments to previous regulations which had been in force since 2003. It gives effect to new provisions which were introduced across the EU by Directive 2009/136/EC and Directive 2006/24/EC. This Office published a guidance note in July 2011 to explain the changes which the instrument introduced.

On the day of the audit, the Inspection Team provided IT Carlow with a copy of a letter which had issued to some 80 organisations nationally relating to SI 336 and, in particular, to Section 6 of the guidance note – Storing and Accessing information on terminal equipment – e.g. "Cookies".

The purpose of the letter is to gather information to assist the Data Protection Commissioner in understanding how organisations are working towards, or have achieved compliance with the revised rules for cookies. These rules are set down in Regulations 5(3) and 5(4) of SI 336 of 2011.

The Office of the Data Protection Commissioner recommends that IT Carlow familiarises itself with this matter and makes provision for its website to be compliant with requirements of the regulation.

3.8 Computer Systems & Security

The Inspection Team met with Fergal Flanagan, Computer Services Manager to discuss the computer systems and security measures, including CCTV, in place in IT Carlow. The Team was informed that IT Carlow has 17 IT staff including 3 or 4 IT staff who operate a helpdesk for the Institute. In terms of overall network security, IT Carlow outlined that it had conducted penetration tests on a server and perimeter security tests had detected no breaches. HEAnet provides the e-Infrastructure service to IT Carlow. IT Carlow outlined that HEAnet is Ireland's National Education and Research Network, providing Internet, associated ICT and e-Infrastructure services to

Educational and Research organisations throughout Ireland. HEAnet's e-Infrastructure services supporting approximately 200,000 students & staff (third-level) and approximately 800,000 students & staff (first and second-level).

3.8.1 Personal Computers

IT Carlow outlined to the Team that it has in the region of 1,500 personal computers across the campus. It was indicated that all PCs have virus protection software installed. Students have their own logon and password in order to access the student systems. Students may access email, the Banner portal and internet. While internet access is logged, it was indicated that usage patterns are not monitored to any great extent. Staff and students are provided with access to personal and public drives on the Institute's systems. As the Institute's systems are accessible to students and staff, separate password policies are in place (see appendix 15) and it was explained that student and staff networks are completely separate.

In relation to 'end of life' computers, it was indicated that the Institute clears down the content of the hard drives and then provides the computers to local schools for use. In the case of older machines, Rehab is contracted to destroy them and the remainder of the pc is then recycled in conjunction with the PC supplier in accordance with the Institute's obligations under the WEEE directive.

3.8.2 Portable ICT Devices

Removable Media

IT Carlow indicated to the Team that by default, CD drives and USB ports are enabled on student computers to facilitate students and staff backing up their data. The Team was informed that there were no plans to disable removable media given the clear demand for such facilities, particularly from academic staff.

The Inspection Team noted that there appears to be wide use of storage devices within the Institute by both staff and students and cautioned that that there is no guarantee that a memory stick, inadvertently used, would not contain a damaging virus. IT Carlow provided the Team with a copy of its **End User Guidelines** policy (see appendix 19) and its **Anti-Virus Scanning and Protection Standard** (see appendix 20) where the topic of portable ICT devices is addressed in detail and the importance of virus protection emphasised along with physical security and controls against unauthorised access to data on portable devices.

Laptops

In relation to laptops, IT Carlow explained that it does not provide laptops to members of academic staff. However, staff members may decide to use their own laptops for business. The Inspection Team asked if staff laptops contain personal data and it was conceded that some staff members' laptops may hold personal data for any number of business reasons. The Institute's IT Acceptable Usage Policy (appendix 16) states that

> "No institute data which is confidential in nature…should be held on Laptops or other storage devices for any longer than is absolutely necessary. Any such data held on these storage devices should be password protected and encrypted."

It was not clear to the Inspection Team on the day of the audit how IT Carlow has oversight in relation to the use of laptops within the institute and the types of data which may be contained on them. Measures such as password protection and encryption should be implemented where personal data is, or is likely to be, stored on laptops or other removable media, but this is a process which should be driven home by the Institute rather than merely requesting staff members to comply with its policies in this regard.

The ODPC recommends that stronger controls are implemented with regard to portable ICT devices area such as checks and reminders to ensure anti-virus and encryption software is in place.

3.8.3 Physical Access

Access to certain staff areas of the Institute is controlled by means of staff swipe-cards. It was indicated to the Team that the data generated by the swipecard is only used for the purpose of the staff member gaining entry to a particular area – it is not used, for example, to record the time a staff member entered or exited a particular area. IT Carlow explained that it has a separate time and attendance system in operation for which staff use a separate swipecard.

3.8.4 IT Policy

It was explained to the Inspection Team that IT Carlow is represented on a working group of IT Managers from each of the Institutes of Technology in Ireland. The working group is currently looking at the standardisation of IT policy across the Institutes with the assistance of Deloitte & Touche.

On the day of the audit, the Inspection Team was provided with a set of policy documents formulated by the working group and currently at draft stage. The ODPC has noted the content of the documents and commends IT Carlow and the working group for the combined approach on these issues. From this Office's point of view, one area of particular concern from a data protection perspective, as highlighted above, is the level of oversight and active intervention which a data controller has in relation to the use of laptop and removable storage devices within an organisation. Going forward, if IT Carlow has any specific questions in relation any data protection aspects of the draft policy documents, the ODPC is happy to provide assistance.

3.9 CCTV

IT Carlow operates an extensive CCTV system across its campus which, it was indicated, is used to deter harassment, assault, theft and vandalism and to assist An Garda Síochána in the investigation of crime. IT Carlow clarified that there are currently 45 internal CCTV cameras and 59 external CCTV cameras in operation at the Institute. The purpose of IT Carlow's CCTV system is set out in its **Security**

Camera Policy (see appendix 17) – namely to promote a safe environment, deter theft and vandalism and assist law enforcement. The policy also states that footage is retained for a period of 6-8 weeks. The Office of the Data Protection Commissioner has issued guidance on its website in relation to the retention of CCTV footage which states that it should be retained for no more than 31 days. Accordingly, it is recommended that IT Carlow brings its retention period in line with this guidance.

In addition, the Team noted that IT Carlow's CCTV policy includes the following wording:

> "From time to time the Institute may investigate alleged breaches of Institute policy by staff. Such investigations may involve misconduct or gross misconduct [as defined in section 11 of the Institute's Disciplinary Procedure]—and in these situations security camera records may be accessed as part of an investigation and managed in accordance with the provisions of the Institute's disciplinary procedure."

Subsequent to the inspection, IT Carlow supplied the Team with a copy of the Institute's Disciplinary Procedure (see appendix 35). Having reviewed the policy, the ODPC noted that first of all that there is no reference in the Disciplinary Procedure document to the use of CCTV in any circumstances where misconduct or gross misconduct is investigated by IT Carlow. Secondly, the ODPC considers that the use of CCTV images for disciplinary purposes raises serious issues of proportionality under data protection legislation. The ODPC refers IT Carlow to a case study published in the Data Protection Commissioner's 2008 Annual Report - Case Study 10: An employer attempts to use CCTV for disciplinary purposes[3]. The case concerned an employer who had used CCTV images to compile a log that recorded employees' pattern of entry and exit from their place of work. The employees complained to the ODPC that they had never been informed of the purpose of the CCTV cameras on the campus where they were employed. The Commissioner in considering this case found that

> "If an employer intends to use cameras to identify disciplinary (or other) issues relating to staff, as in this instance, staff must be informed of this before the cameras are used for these purposes… Transparency and proportionality are the key points to be considered by any data controller before they install a CCTV system. Proportionality is an important factor in this respect since the proposed use must be justifiable and reasonable if it is not to breach the Data Protection Acts. Notification of all proposed uses will not be enough if such uses are not justifiable."

The ODPC advises IT Carlow that the findings of the Commissioner in the case above should be reflected in IT Carlow's usage of CCTV footage and general guidance on CCTV[4] issued by the ODPC followed in this regard also.

The Inspection Team examined the CCTV monitor which controls the system and noted that it is accessible to six named individuals including the Computer Services Manager by means of a specific system password. The ODPC advises IT Carlow that safeguards in terms of access to the system should be reviewed including the creation

[3] http://www.dataprotection.ie/viewdoc.asp?m=p&fn=/documents/annualreports/AR2008.pdf
[4] http://www.dataprotection.ie/docs/Data-Protection--CCTV/242.htm

of passwords that require the unique log-in of the staff member. The Team was informed that the CCTV system covers the campus both internally and externally and that the cameras are generally focused on exits and stairwells. This was confirmed following the examination of the camera monitor. However, the Team did request to look at 6 cameras in particular, which are located in the Student Union Common Area (3), the gym (2) and the high performance gym (1). In these instances the cameras do not focus on exits or stairwells, but clearly capture the day to day activities of students (and staff) that happen to be in these areas.

The ODPC advises IT Carlow that images captured by CCTV cameras are personal data within the meaning of the Data Protection Acts and are subject to the provisions of the Acts. Use of CCTV cameras must be proportionate and transparent - see **Case Study 3 in 2007 Annual Repor**t **–** and in the case of gyms and leisure centres where it is decided by the data controller that the use of CCTV is warranted (and they can adequately demonstrate so if this use is questioned) all of the purposes should be included in the signage. For example, if there is CCTV in place for insurance purposes this should be explicitly stated.

The ODPC recommends that signage should be erected in all of these areas without signage to show that CCTV is in operation, stating the specific purpose(s) for which CCTV is in operation. The signs should also include the contact details of the data controller.

[redacted]

[redacted]

[redacted]

[redacted]

4. FINDINGS

Excellent co-operation was received throughout the inspection itself. The Inspection Team considered that there was good organisational awareness of data protection principles generally. In addition, IT Carlow supplied the Team both before and during the inspection with a comprehensive set of policy documents relating to data protection issues and data security.

The ODPC considers that the use of CCTV images by IT Carlow for disciplinary purposes raises serious issues of proportionality under data protection legislation and it is recommended that IT Carlow review its overall HR policy as well as its CCTV policy in this regard taking into account Case Study 10 of the Data Protection Commissioner's 2008 Annual Report.

[redacted]

With regard to disability and financial supports and services, the ODPC is satisfied that data collected is not excessive and is in line with requirements across the sector. However, caution is advised with regard to all processing such data which is sensitive data under the Data Protection Acts. In addition, the security of such data is a paramount and access must be predicated on a need-to-know basis at all times.

Overall, the ODPC has for some time had concerns regarding information flows within the higher education sector which ultimately when connected with other datasets may allow individuals to be identified. This is a matter which will be re-examined by the ODPC.

The Commissioner would like to thank all the staff of IT Carlow for the co-operation and assistance provided to the Inspection Team on the day.

5. RECOMMENDATIONS

5.1 Obtaining and Processing of Personal Data

- It is recommended that IT Carlow's enrolment form is amended to state the reasons for which the PPSN is being sought (HEA returns and Department of Social Protection anti-fraud checks).

- It is recommended that the PPSN is masked on Banner with access to the full PPSN visible only to the staff submitting the returns to the HEA and Department of Social Protection.

  [Since the inspection took place, IT Carlow has indicated that it will put a mechanism in place which will mask the PPSN in Banner].

- It is recommended that IT Carlow contacts Client Identity Services in the Department of Social Protection with a view to amending its entry on the register of PPSN users in light of its collection of student PPSNs for the purposes of submitting returns to the Department and the HEA.

- It is recommended that all application forms and the enrolment form include a tick box in order to allow a student to opt out of having his or her image further processed by IT Carlow.

5.2 Disclosures of Data

- In relation to requests from An Garda Síochána over the telephone, it is recommended that all such requests be followed up in with a written copy of the request on AGS headed paper signed by the District Superintendent and that a log of all such requests received is maintained by IT Carlow.

5.4 IT Carlow Website

- It is recommended that IT Carlow familiarises itself with SI 336 of 2011 in relation to the provision of ‘cookie’ information for customers on its website and ensures that it becomes compliant with the regulations.

5.5 Computer Systems & Security

- It is recommended that stronger controls are implemented in the area of portable ICT device security.

5.6 CCTV

- The ODPC considers that the use of CCTV images for disciplinary purposes raises serious issues of proportionality under data protection legislation and it is recommended that IT Carlow review its overall HR policy as well as its CCTV policy in this regard.

- It is recommended that CCTV footage is retained for no longer than 31 days.

- It is recommended that signage should be erected in the Student Union Common Area, the gym and the high performance gym to show that CCTV is in operation and stating the specific purpose or purposes for which CCTV is in operation. The signs should also include the contact details of the data controller.

- Safeguards in terms of access to the CCTV monitoring system of IT Carlow should be reviewed including the creation of passwords that require the unique log-in of the staff member.

6. APPENDICES

Appendix 1	Letter of Intention to Audit
Appendix 2	Enrolment Form
Appendix 3	Lifelong Learning Application
Appendix 4	Banner Screenshots
Appendix 5	Banner logon notice
Appendix 6	European Diploma Supplement
Appendix 7	HEA Access Survey Leaflet
Appendix 8	Access Survey Screenshots
Appendix 9	CAP Disability Entry Programme application
Appendix 10	Letter to CAP applicants re disclosure of disability
Appendix 11	CAP Financial Supports Application
Appendix 12	SAF Funding Application
Appendix 13	Student Handbook
Appendix 14	Records Retention Schedule
Appendix 15	Computer Password Policy
Appendix 16	IT Acceptable Usage Policy
Appendix 17	Security Camera Policy
Appendix 18	Biometrics – roles and responsibilities
Appendix 19	End User Guidelines Policy
Appendix 20	Anti-Virus Scanning and Protection Standard
Appendix 21	Acceptable Usage Policy (different to appendix 16)
Appendix 22	Information Security Policy
Appendix 23	Data Governance Policy
Appendix 24	Compliance Policy