Code of Practice

for the

Protection of Personal Data

in

Vocational Education Committees

Chief Executive and Education Officers' Association

Cumann na bPríomh Oifigeach agus Oifigeach Oideachais

Contents

1. Foreword

I am very happy to be able to formally approve this Code of Practice under the terms of Section 13 of the Data Protection Acts 1988 and 2003. The Code is the result of intensive work by the Vocational Educational Committees and their staff, working in close co-operation with my Office. It is designed to give operational meaning to the principles of data protection set out in European and National law.

I am confident that the Code will make a significant contribution to improving knowledge and understanding of data protection within the Vocational Education Committees. I intend to continue to work closely with the Vocational Education Committees and their staff to ensure that the guidance set out in the Code is followed in daily practice.

Billy Hawkes
Data Protection Commissioner

20 August 2012

2. Introduction

Vocational Education Committees are statutory authorities which have responsibility for vocational education, training, youth work and a range of other statutory functions. VECs also manage and operate post-primary schools, further education colleges, community primary schools and a range of adult and further education centres delivering education and training programmes to all sectors of the communities served by the VECs.

Data (including information and knowledge) is essential to the administrative business of Vocational Education Committees (VECs). In collecting personal data, the VEC has a responsibility to use it both effectively and ethically. There is a balance to be struck between an individualôs right to privacy and the legitimate business requirements of the VEC. Therefore, it is critical that VEC staff work to the highest standards. Our integrity includes both the way in which we conduct ourselves and the way in which we ensure the data we hold is compliant with relevant legislation.

The responsibility for data protection is an onerous one which requires a commitment to regular and clear action. This code helps all of us to decide on what needs to be done, who needs to do it and how it needs to be done.

VECs have always been very careful to keep records safely and to ensure that access to records is restricted to those with authority. In recent times, data has been stored differently and with the advent of off-site storage and the ability to access archives remotely, our processes require more vigilance. As responsible public bodies, VECs respect the highest standards of data protection. The code helps us all to ensure that we can remain safe organisations in relation to the data we hold.

Set against the Data Protection Acts 1988 and 2003 the aim of this Code of Practice is to ensure each employee of the VEC has an understanding of the concepts of Data Protection and is aware of their own responsibilities. This, in turn, will assist the VEC in its compliance with the Acts.

Protecting our data is common sense. We need to ensure that data gathered and processed by the VEC is compliant with Data Protection Legislation. Reading and understanding of the code by all employees will go a long way towards meeting this requirement.

Further advice in relation to the storage, handling and protection of personal data is available from the Data Protection Commissionerôs website.

Paddy Lavelle
President of CEEOA
26 July 2012

3. Legal basis for collecting and retaining personal data

The VECs were established under the Vocational Education Act 1930. The Act was amended in 1936, 1944 and 1970; however a major overhaul of the legislation came with the Vocational Education (Amendment) Act 2001. Other legislation which places obligations and responsibilities on VECs include: the Education Act 1998, the Education (Welfare) Act 2000, and the Youth Work Act 2001.

In performance of its statutory duties, the VEC collects and retains personal data. Some of the legislation governing the operation of VECs and those provisions which relate to data protection are as follows:

Vocational Education Acts 1930 - 2001

- S.30 Duties generally of VECs
- S. 31 Duty to prepare and submit to the Minister a scheme setting forth the general policy of the VEC
- S. 32 Establish and maintain continuation schools in its area; establish and maintain in its area courses of instruction in the nature of continuation education; assist in maintaining schools in its area in which continuation education is provided.
- S. 33 Duty to ñregister and classifyò young persons with prospects of employment in trade etc.
- S. 7 Composition of vocational education committees
- **S. 9 2001 VE Acts Functions of VECs**
    - (*a*) plan, coordinate and review the provision of education and services ancillary thereto in recognised schools and centres for education
    - (*b*) assess whether the manner in which it performs its functions is economical, efficient and effective,
    - (*c*) adopt and submit an education plan,
    - (*d*) adopt and submit a service plan
    - (*e*) make all reasonable efforts to consult with:
        - (i) boards of management,
        - (ii) similar persons to boards of management,
        - (iii) students registered at such schools or centres for education,
        - (iv) parents of students who are so registered and who have not reached the age of 18 years,
        - (v) members of the staff, and
        - (vi) such other persons as it considers are likely to be affected as a result of the performance by it of its functions, or as it considers have a particular interest or experience in relation to the education or training provided in recognised schools or centres for education established or maintained by it

- (*f*) in the performance of its functions and in so far as is practicable, cooperate with other vocational education committees, schools and such persons providing services similar to or connected with those provided by the vocational education committee concerned in relation to the vocational education area of that committee as the VEC considers appropriate.

- Elections to VECs are conducted under the regulations contained in the Composition of Vocational Education Committee Regulations 2004 (SI 924/2004) of which the following are the relevant points:
  Reg. 2 (the interpretation section):
  ñelectionò refers to elections under section 8-(1)(c) or (d) or 8-(2)(b) or (c) of the Principal Act (i.e. elections of parentsô or staff representatives);

  Reg. 4: The Minister is obliged to appoint a returning officer;

  Reg. 6: *(1)* duty of returning officer: on appointment ñshall cause to be prepared a provisional electoral roll containing the names and addressed of each eligible parentò;
  (3) returning officer must make this roll available for inspection ñin the manner the retuning officer considers appropriateò;

  Reg. 7: ñThe electoral roll of eligible parents shall contain the name and address of every eligible parent who qualifies to be entered on the rollò.

- Under Section 9(g) of the Education Act, 1998, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the School relating to the progress of the student in his or her education.

- Under Section 20 of the Education (Welfare) Act, 2000, the School must maintain a register of all students attending the School.

- Under Section 21 of the Education (Welfare) Act, 2000, the School must record the attendance or non-attendance of students registered at the School on each School day.
- Under Section 28 of the Education (Welfare) Act, 2000, the School may supply *Personal Data* kept by it to certain prescribed bodies provided the School is satisfied that it will be used for a ñrelevant purposeò.

Youth Work Act 2001

- **9.**(1) In addition to the functions conferred on it by or under the VE Acts, 1930 to 2001, each VEC shall, as far as practicable and within the financial resources available to itð
- (*a*) ensure the provision within its vocational education area of youth work programmes or youth work services, or both, by:
  - (i) co-ordinating its plans, proposals and activities with approved national voluntary youth work organisations, designated local voluntary youth work organisations and authorised organisations within its vocational education area so as to ensure the provision of those programmes and services by those organisations, and
  - (ii) providing assistance, including financial assistance, to [such organisations]

- (*b*) ensure co-ordination within its vocational education area of youth work programmes and youth work services with education programmes and other programmes that provide services for young persons,
- (*c*) ensure that in the provision of youth work programmes or youth work services, or both, under *paragraph (a)*, particular regard shall be had to the youth work requirements of:
    - ï (i) persons who have attained the age of 10 years but not 21 years, and
    - ï (ii) other young persons who are socially or economically disadvantaged,
- (*d*) without prejudice to *section 8(1)(e)* and *(g)*, monitor and assess the youth work programmes or youth work services, or both, for which moneys are provided under this section and in particular shall have regard to an evaluation of the expenditure incurred in the provision of such programmes or services,
- (*f*) consult with and report to, in regard to youth work, such person or persons as the Minister may, from time to time, direct.

Some of the relevant legislation which places an obligation on the VEC to obtain and retain personal data:

- The Teaching Council Act 2006
- Social Welfare Acts
- Minimum Notice & Terms of Employment Act 1973
- Payment of Wages Act 1979
- Pensions Acts 1990-2003
- Comptroller & Auditor General Act 1993
- Maternity Protection Acts 1994-2004
- Organisation of Working Time Act 1997
- Parental Leave Acts 1998-2006
- Carers Leave Act 2001
- Adoptive Leave Act 2005
- Safety, Health & Welfare at Work Act 2005
- Various Taxation Legislation

The VEC is also regulated by Circular Letters and Memos issued by the Department of Education and Skills. These regulations require personal data to be collected, retained by the VEC and in some cases data is to be transferred to DES.

4. Responsibility for Data Protection

The Chief Executive Officer of each VEC has overall responsibility for Data Protection. Delegated officers of the VEC i.e. Principals, Centre Managers, Programme Co-ordinators, Education Officers and Assistant Principal Officers are also responsible; however, all employees share responsibility for data protection in their own area of work.

5. Registration with the Office of the Data Protection Commissioner

As a public body, each VEC is required to register with the DPC as a Data Controller. This registration will detail the name and contact details of the data controller, the purpose for collecting data, a description of the data collected, a list of any disclosees and whether or not data is transferred abroad. This registration is renewed annually at which time the VEC will review their registration details and update where necessary.

6. Policy

The VEC will have policies and procedures in place relating to data protection and retention of personal data. These policies and procedures will include:

- Data Protection Policy
- ICT Acceptable Usage Policy
- CCTV Policy
- Records Management /Records Retention Policy
- Breach Management Policy (template available at Appendix 4)

These will be reviewed regularly in light of changing legislation and business needs.

7. Code of practice relating to data protection rules

The Data Protection Acts 1988 and 2003 confer rights on individuals as well as responsibilities on those persons controlling and processing personal data. The VEC has key responsibilities in relation to the information which it keeps on computer or in structured manual files about individuals. The VEC undertakes to execute its responsibilities in accordance with the eight Data Protection Principles/Rules as outlined below:

7.1. Obtain and process the information fairly

The VEC will ensure that data subjects are aware, at the time the personal data is being collected, of the identity who is collecting it, the purpose for collecting it, how the data will be used, the categories of persons to whom the data may be disclosed and any other information which is necessary so that processing is fair. In most cases individuals will have consented to the collection of their data by the VEC either because they have applied for a job with the VEC, enrolled as a student or applied to participate in some other VEC service or for the performance of a contract.
Where required, in accordance with the Data Protection Acts consent will be sought for the processing of personal data and in particular, explicit written consent will be sought for the processing of sensitive data.

The following are details of type of personal data which are held by the VEC, and the purpose(s) for collecting the data in each case:

(a) Employee Records

The VEC holds some or all of the following information about its employees:

Name, address, date of birth, PPS Number, marital status, educational or previous employment background, history with the VEC and details of current position, CVs, applications and interview records, references, performance reviews, salary, CCTV images, records of disciplinary investigations/meetings or grievances, pension and other insurance documentation, payroll details, bank details, details of absences, disclosures of interest.

This information is required for routine management and administration of contracts of employment and to protect employeeôs rights under various employment laws.

Sensitive Personal Data

Certain categories of information are categorised as ñsensitiveò under data protection legislation. The VEC may hold some or all of the following sensitive information about its employees:

- **Information about racial or ethnic origin.** *The VEC may hold this information for statistical purposes only.*
- **Medical information, including the medical questionnaire which employees complete prior to taking up employment, records of sickness absence and medical certificates.** *The VEC is required by DES to request all employees to have a medical examination and will therefore hold the resulting medical report. The purpose of keeping this sort of information is to administer sick pay and disability entitlement, monitor and manage sickness absence and to comply with health and safety obligations. Satisfactory health is one of the conditions of admission to the Superannuation Scheme.*
- **Information regarding Trade Union membership.** *The VEC holds this information for the purposes of facilitating the deduction-at-source of union subscriptions only.*
- **Information on commission/alleged commission of offence, any proceedings for an offence.** *The VEC holds this information to meet the requirements of the Department of Education & Skills and to satisfy itself of the employee's suitability for their position* in *relation to child protection.*
- **Information regarding disability**. *The VEC holds this information for the purposes of reporting to the Department of Education and Skills on the target for employment of persons with disability under the Disability Act 2005.*

(b) Student Records

The VEC obtains, processes and holds personal data of the following categories of students and the parents/guardians of students aged under 18 years:

- *students attending second-level VEC schools*
- *students attending VEC centres of education e.g. Youthreach, FE Colleges, Prison Education Services, Traveller Training Centres*
- *students enrolled on VEC courses and programmes e.g. BTEI, VTOS, Community Education*
- *primary level students where the VEC is patron of a primary school.*

The personal data may include:

- **Information which may be sought and recorded at enrolment, including: name, address, date of birth and contact details, PPS number where a basis exists for its collection; names and addresses of parents/guardians and their contact details.**

- **Sensitive personal data which may include: religious belief; racial, ethnic or national origin; membership of the Traveller community, where relevant; any relevant special conditions (e.g. special educational needs, health issues etc.) which may apply.**
- **Information on previous academic record, psychological assessments, attendance records, academic record – subjects studied, class assignments, examination results as recorded on official school reports, records of significant achievements, records of disciplinary issues and/or sanctions imposed, other records e.g. records of any serious injuries/accidents etc**.

The purpose for collecting, processing and retaining this information is, to enable each student to develop his/her full potential, to comply with legislative or administrative requirements, to ensure that eligible students can benefit from the relevant additional teaching or financial supports, to support the provision of religious instruction, to enable parent/guardians to be contacted in the case of emergency etc.

Each year, in October, each recognised post primary school makes a return to the Department of Education and Skills, the data from which allow the DES calculate the teaching posts and core funding to be allocated to each recognised post primary school, for the following school year.

These returns are made in accordance with ***The Rules and Programme for Secondary Schools*** via a process called the *Annual Post-Primary School October Return/Examination Entries,* or more familiarly known as the October Returns. In making their respective returns to the Department, post primary schools transfer personal data and personal sensitive data on each of their enrolled students. The only purpose some post primary schools may collect some of these data is to meet the data requirements for their October Return to the Department.[1]

Sensitive Data which may be sought at the time of enrolment includes membership of the travelling community and medical card information. This information is sought and retained for the purpose of completion of the October Returns. Explicit consent will be sought from parents/guardians before processing this data in line with DES C/L 47/2010.

The VEC holds some or all of the following information about students and parents/guardians who are applicants for grants and scholarships:
Name, address, date of birth, examination results, details of parent/guardian's PPS Number, marital status, details of employment, salary/income details, bank details, and other documentation relating to applications for grants/scholarships.
This information is required for assessing eligibility for grant/scholarship, the processing of applications and the routine administration of the grant/scholarship schemes.

The VEC runs a number of out of school classes and summer camps for children of various ages who may or may not be enrolled at VEC schools. These may include Music Classes; Summer Camps e.g. Outdoor Education, Sports, Art, Computer, Drama, Music and Cookery. Camps and classes are held in VEC schools and centres and other appropriate locations. The VEC will obtain, process and hold some or all of the following personal data about participants and their parents/guardians:

[1] DES Circular Letter 0047/2010 Fair Processing of Student Personal Data

Name, address, date of birth, contact details for parent/guardian, details of relevant medical conditions

This information is required for the processing of applications and the routine administration of the activities**.**

(c) Committee/Boards of Management Records

The VEC holds some or all of the following information about Committee members, members of Boards of Management:

Name, address, contact details, records in relation to appointments to the Committee/Board of Management, minutes of meetings and correspondence, travel expenses paid, PPS Number, tax details, bank details.

This information is required for routine management and administration Committee/Boards of Management business, payment of allowances and expenses and to document decisions made.

(d) VEC Register of Electors

Under the Vocational Education Amendment Act 2001, *"2 members elected by parents of students who have not reached the age of 18 years and who are registered as students at recognised schools or centres for education established or maintained by that Committee,"* and *"2 members elected by members of staff of that Committee,"*. Elections are held every 5 years and the Administration Centre Staff prepare a Provisional Electoral Roll from a list of parents provided by the schools. Co Monaghan VEC holds some or all of the following information about electors:

Name, address, completed ballot paper

This information is required for the preparation of the provisional and final electoral rolls, the distribution of ballot papers and to maintain a record of the election of parent and staff representatives to the Committee.

(e) Creditors

The VEC holds some or all of the following information about creditors (some of whom may be self-employed individuals):

Name, address, and contact details, PPS Number, disclosures of interest, tax details, bank details and amount paid.

This information is required for routine management and administration of the VECôs financial affairs including the payment of invoices and compliance with taxation regulations.

(f) CCTV Images/Recordings

CCTV (Closed Circuit Television) is installed in some of the Committeeôs schools, centres and offices, externally i.e. perimeter walls/fencing and internally as detailed in the CCTV policy. These CCTV systems may record images of staff, students and members of the public who visit the premises.

This personal data is obtained (i.e. recorded) for the Safety and security of staff, students and visitors and to safeguard VEC property and equipment. Cameras are located externally and internally and recording equipment is located in the Principal/Managerôs office or in the reception office of each school or centre. Access to images/recordings is restricted to the Principal & Deputy Principal of each school and Manager of each centre. Tapes, DVDs, hard disk recordings are retained for 28 days, except if required for the investigation of an incident. CCTV systems will be operated in accordance with the VEC CCTV Policy.

A list of all information, including sensitive information, which the VEC holds on each individual, is available to that individual on request from the Chief Executive Officer.

7.2. Keep it only for one or more specified, explicit and lawful purposes

The VEC will keep data for purposes that are specific, lawful and clearly stated and the data will only be processed in a manner compatible with these purposes. The VEC will state at the point of data capture (enrolment forms, application forms, customer service forms, website) the purpose for collecting the information, that the information will be processed and kept only in a manner which is compatible with this purpose and that the obtaining, processing and retention of such information will be done so in line with the Data Protection Acts. In particular, the VEC will be careful in its use of the PPS Number in systems, on forms and documentation. There is a strict statutory basis providing for the use of the PPSN and the VEC is registered with the Department of Social Protection for the use of PPSN. This allows organisations use the PPSN in support of a provision of a public service to a customer. The PPSN will only be used where there is a legitimate reason for doing so. The legal basis for holding personal data is set out in section 3 above.

7.3. Use and disclose it only in ways compatible with these purposes

The VEC will only use and disclose personal data in ways that are necessary for the purpose/s or compatible with the purpose/s for which it collects and keeps the data.

For the purposes outlined at 1 & 2 above, it may from time to time be necessary to disclose data subjectôs personal data to third parties. The restriction on processing of personal data (including disclosure to a third party) is lifted in a limited number of circumstances. These circumstances are specified in Section 8 of the Data Protection Acts. The VEC will ensure that any requests for disclosure of personal data under Section 8 of the Acts are received in writing. The data subject will be informed of these disclosures at the time of obtaining the data via data protection notices on application form, enrolment forms etc. The VEC will ensure, by way of implementing a specific disclosure policy, that staff/department involved in processing personal data are aware of the purpose of collecting such data and use/process it only for that specific purpose or compatible purpose/s.

Where a data subject has been informed of the potential disclosure or where consent has been collected, it may then be acceptable to disclose relevant personal information to entities such as those listed below. Where consent is not in place, the VEC understands that it must have a legal basis for disclosing an individualôs information.

- Employeeôs personal data may be disclosed to: **the Department of Education & Skills, Revenue Commissioners, Department of Social Protection, the Central Statistics Office, the Teaching Council, other educational institutions, banks and other financial institutions, past and future employers, auditors (C & AG and VSSU), pension administrators, An Garda Síochána, trade unions and staff associations.**
- Studentôs and parent/guardianôs personal data may be disclosed to: **The Department of Education & Skills, (which includes the Inspectorate the State Examinations Commission and the National Educational Psychological Service (NEPS), the National**

Council for Special Education (NCSE), the National Educational Welfare Board (NEWB), Bus Éireann (re school transport) the Health Service Executive, An Garda Síochána.

- It may also be necessary to disclose information in order to comply with legal and statutory obligations.

Transfer of personal data will be compatible with the original purpose for obtaining such data and if it is not, consent for transfer will be sought. The VEC takes all reasonable steps as required by law to ensure the safety, privacy and integrity of the information and, where appropriate, will enter into contracts with such third parties to protect the privacy and integrity of any information supplied. The VEC will endeavour to comply with the guidance in relation to the transfer of personal data outlined in the Department of Finance ñGuidance Note on Protecting the Confidentiality of Personal Dataò ï December 2008 (Appendix 3).

Where transfer of data is requested is not of a routine nature and is not listed above, VEC staff will consult with the CEO before proceeding.

Where an external Data Processing company is used e.g. computerised processing of payroll, the VEC will have a written contract with the company in place which details the data to be processed, how long data is to be stored, what the company may do with the data; what security standards should be in place and what verification procedures may apply.

7.4. Keep it safe and secure

The VEC stores all personal information in controlled access, centralised databases (including computerised and manual files) at its Administrative Offices and in the offices of its schools and centres. The VEC will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. The VEC acknowledges that high standards of security are essential for processing all personal information. The VEC will undertake to implement the guidance in relation to the storage, handling and protection of personal data contained in the Department of Finance ñGuidance Note on Protecting the Confidentiality of Personal Dataò ï December 2008.

The high standards of physical and technical security are essential to protect the confidentiality of personal data and will be implemented by the VEC. These include, inter alia:

- Ensuring access to information is restricted to authorised staff in accordance with the VEC ICT Acceptable Usage Policy and other related VEC policies and procedures.
- Ensuring computer systems are password protected. A strong password should include a minimum of twelve characters and contain one or more Letters, Symbols, Numbers, and possibly also punctuation.
- Vendor supplied defaults for system passwords and other security parameters are never be left in place.
- Keeping information on computer screens and paper files hidden from callers to offices
- Staff members are required to lock their computers when leaving their work stations and to log out of the computer system and lock away paper files containing personal data at the end of each day. Automatic Time-Out should occur where system terminals are idle for a pre-defined time period.
- Audit logs will be kept in relation to changes, additions and deletions to specific data on key ICT systems. Senior Management and CEO, in co-operation with the IT Systems

Administrator, will assess the requirement to monitor access to applications with personal data to ensure that appropriate monitoring is undertaken in accordance with the VEC ICT Acceptable Usage Policy.

- Ensuring that personal data is protected by strong encryption when being stored on portable devices or transferred electronically (including via email).
- Ensuring that personal data is not stored on portable devices except in essential circumstances. Where deemed essential, data will be encrypted and a record kept of the nature and extent of the data and why it is being stored on a portable device. Arrangements will be put in place to fully delete the data on the portable device when it is no longer being used.
- Having appropriate facilities in place for secure disposal of confidential waste.
- Having appropriate procedures in place for the disposal of computer equipment, i.e. Hard-Drives, Servers, Storage Disks, etc. These procedures must ensure the satisfactory deletion or removal of all relevant data.
- Non-disclosure of personal security passwords to any other individual (including other employees)
- Automatic Password Change requirement at pre-set intervals. This ensures that passwords which have been disclosed to part-time or temporary staff will have a limited life-span.
- Automatic recording and notification of User-IDs and Passwords which have been inactive for a pre-defined time-period.
- Keeping premises secure, especially when unoccupied
- A network based Intruder Detection System (IDS) that acts as an internal alarm system and monitors and reports on malicious activities on a network or system.
- Appropriate Anti-virus software to prevent infection from the internet (either e-mail or web-sourced) and also to prevent viruses that may also be introduced from internal portable devices, such as memory sticks (the use of which should be strictly limited).
- Appropriate firewall protection where there is external connectivity, either to other networks or to the internet. Firewalls must be properly configured to maximise protection from malicious intrusion.
- Having adequate security measures and policies in place in relation to the use of laptops and other mobile storage devices
- Having strict protocols in place for remote access to data held on VECs servers
- Restricting access to CCTV systems and recordings in accordance with the CCTV policy
- Appropriate data protection and confidentiality clauses will be in place in contracts with any third party acting as a processor of personal data on behalf of the VEC

Responsibility for the above will be assigned to named person(s) in each of the VECs. All members of staff are required to meet these standards and periodic reviews of the measures and practices in place will be carried out by management.

7.5. Keep it accurate and up-to-date

The VEC will have procedures in place that are adequate to ensure high levels of data accuracy and completeness and to ensure that personal data is kept up to date. These procedures include:

- Cross-checking of data entry e.g. entering pay details onto payroll system requires one person to enter the data while another person checks for accuracy
- Files (electronic and manual) are audited periodically by the internal auditors the Vocational Support Services Unit (VSSU) and the Comptroller & Auditor General (C& AG)

The VEC relies on the individuals who supply personal information (staff, students and others) to ensure that the information provided is correct and to update us in relation to any changes to the information provided. Notwithstanding this, under Section 6 of the Data Protection Acts, individuals have the right to have factual personal information corrected if necessary. If an individual feels that the information held in incorrect they should write to the CEO. The VEC will reply to such a request within 40 days detailing either the confirmation of the rectification or erasure, or a full explanation as to why the request is being refused.

7.6. Ensure that it is adequate, relevant and not excessive

The VEC will ensure that information sought and retained is the minimum amount needed for the specified purpose and is adequate, relevant and not excessive in relation to the purpose(s) for which it is kept. The methods of collecting personal information will be subject to periodic review to assess the continued need for information sought.

7.7. Retain it no longer than is necessary for the specified purpose or purposes

The VEC will develop a defined policy on retention periods for personal data and appropriate management, clerical and ICT procedures in place to implement such a policy.
Retention times cannot be rigidly prescribed to cover every possible situation and the VEC will exercise judgement, taking account of statutory obligation and best practice in this regard in relation to each category of records held. However, the following particular requirements should be met:

- School registers and roll books are required to be kept indefinitely within the School.

- Pay, taxation and related employment records should be retained in accordance with the time periods set out in various Acts and Statutory Instruments governing taxation and employment law.

- Where litigation may potentially arise in the future (e.g. in relation to accidents/personal injuries involving employees/students or accidents occurring on VEC property), the relevant records should be retained until the possibility of litigation ceases.

  Note: The statute of limitations in relation to personal injuries is currently two years. The limitation period for other causes of action varies, but in most cases is not greater than six years. A limitation period does not begin to run until the person concerned acquires knowledge of the facts giving rise to the claim. In the case of minors, the limitation period does not begin to run until they reach their 18th birthday or later if the date of knowledge post dates their 18th birthday. While Schools may wish to draw up their own policies as to

how long to retain such records, it would appear prudent not to destroy records likely to be relevant in litigation at least until the **six year limitation period** has expired.

In line with the above, it is suggested that the information on student files might, as a general rule, be retained for a period of six years after the student has completed the Senior Cycle and/or reached the age of 18.

Personal data which is no longer required to be retained will be disposed of securely i.e. paper files confidentially shredded, disks wiped clean before disposal. A destruction certificate will be retained giving a brief description of the data, date of destruction and rationale for destruction.

7.8. Give a copy of his/her personal data to any individual, on request

Individuals have the right to periodically review, update and/or correct their personal information held by the VEC. The right of access does not include a right to see personal data about another individual, without that other personôs consent. Should an employee, Committee member, member of a Board of Management, student, parent/guardian or creditor wish to access their personal information they should contact the Chief Executive Officer in writing stating that they are making an access request under section 4 of the Data Protection Acts and giving any details which might be needed to help identify him/her and locate all the information the VEC may keep about him/her. A maximum fee of ú6.35 may be charged for accessing the data

A copy of the information requested will be provided within 40 days of receipt of such request (60 days in the case of examinations data), in accordance with the Data Protection Acts 1988-2003. If an access request is being refused, the VEC will clearly state the reasons for refusal (as per exemptions in Sections 4, 5 and 8 of the Data Protection Acts[2]).

The Freedom of Information Act does not currently extend to Vocational Education Committees; however the following should be noted for future reference. Where a request is made to the VEC by, or behalf of, a person seeking access to their own personal information under the Freedom of Information Act, the VEC will write to the requestor and inform her/him that the VEC does not currently come under the provisions of the Freedom of Information Act and that their request is being treated as an Access Request for Personal Data Section 4 of the Data Protection Acts. The VEC may seek additional information from the individual making the request in order to assist with locating the personal information requested. Guidance on how organisations should deal with the overlapping rights of individuals is contained in the Freedom of Information Central Policy Unit Notice Number 23 which is available at http://www.foi.gov.ie/cpu-notices.

[2] 1 Under Section 3 of the Data Protection Acts, an individual has a separate right to be informed whether an organisation holds personal data on him/her and, if so, to be given a description of the data and the purposes for which they are kept within 21 days of making the request. The restrictions on the right of access to data which are set out in Sections 4 and 5 of the Acts do not apply to the Section 3 right.

8. Responsibility of Employees of the VEC

All employees of the VEC have a duty to ensure compliance with the principles of Data Protection and undertake to follow the provisions of this Code of Practice in accordance with the VECôs policy and procedures. The VEC will provide information, training and support for employees to ensure compliance with this Code of Practice and the Data Protection Acts.

All employees are charged with the responsibility of ensuring that all data that they access, manage and control as part of their daily duties is carried out in accordance with the Data Protection Acts and this Code of Practice.

Employees found in breach of the Data Protection rules may be found to be acting in breach of or, in certain circumstances, committing an offence under the Data Protection Acts 1988 and 2003. All current and former employees of the VEC may be held accountable in relation to all data processed, managed and controlled by them during the performance of their duties in the organisation.

9. Audits of data protection and code of practice procedures within the VEC

Internal Audits in VECs (with the exception of City of Dublin VEC) are conducted by the Vocational Support Services Unit (VSSU). The Steering Committee of the VSSU together with the Audit Committees of individual VECs, when determining, in consultation with CEOs, the work programme of the VSSU, will ensure that the programme contains adequate coverage by the VSSU of areas within their organisations which are responsible for the storage, handling and protection of personal data. The particular focus of any review by the VSSU would be on assessing the adequacy of the control systems designed, in place and operated in these areas for the purpose of minimising the risk of any breach of data protection regulations. Risks associated with the storage, handling and protection of personal data will be included in the VECôs risk register and risk assessments will take place as part of the VECôs risk strategy exercise. Furthermore, external audits of all aspects of Data Protection within the organisation may be conducted on a periodic basis by the Office of the Data Protection Commissioner.

External Audits of VECs are conducted by the office of the Comptroller and Auditor General (C & AG) on an annual basis.

10. Protocol for reporting breaches

If any breaches of the code of practice or of the regulations in the Data Protection Acts are committed, the Principal, Centre Manager or Programme Co-Ordinator should notify the CEO. The CEO will then decide what action should be taken: whether the breach warrants notification to the Office of the Data Protection Commissioner; whether the individual needs to be notified; whether other third parties (e.g. DES, Gardaí) need to be notified; and how notification should be managed in accordance with the Data Protection Commissioners Personal Data Security Breach Code of Practice. Specifically Paragraph 6 of the Code states:
ñAll incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner as soon as the data controller becomes aware of the incident, except when the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) and it affects no more than 100 data subjects and it does not include

sensitive personal data or personal data of a financial nature. In case of doubt - in particular any doubt related to the adequacy of technological risk-mitigation measures - the data controller should report the incident to the Office of the Data Protection Commissioner.ò http://www.dataprotection.ie/docs/Breach_Notification_Guidance/901.htm

Each VEC should have in place a Breach Management Policy/Plan. A template policy is available at Appendix 4.

Further information in relation to breach notification procedures is available in the Department of Finance Guidance Note on protecting the confidentiality of personal data (Appendix 3).

Appendix 1

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the code of practice;

The Data Protection Acts ï The Data Protection Acts 1988 and 2003 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All VEC staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation

Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (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).

Relevant Filing Systems - Any set of information organised by name, PPS Number (if applicable in an organisation), payroll number, employee number, student number or date of birth or any other unique identifier would all be considered relevant.

Personal Data ï 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.

Sensitive personal data - relates to specific categories of data which are defined as data relating to a personôs racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership. Individuals have additional rights in relation to the processing of any such data.

Access Request ï this is where a person makes a request to the organisation for the disclosure of their personal data under section 4 of the Acts.

Data Processing - performing any operation or set of operations on data, including:

- Obtaining, recording or keeping the data,
- Collecting, organising, storing, altering or adapting the data,
- Retrieving, consulting or using the data,
- Disclosing the data by transmitting, disseminating or otherwise making it available,
- Aligning, combining, blocking, erasing or destroying the data.

Data Subject ï an individual who is the subject of personal data.

Data Controller - a person who (either alone or with others) controls the contents and use of personal data.

Data Processor - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of his/her employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Act places responsibilities on such entities in relation to their processing of the data.

Appendix 2

Enforcement of data protection legislation

Data Protection Commissioner

The Data Protection Acts established the independent Office of the Data Protection Commissioner. The Commissioner is appointed by Government and is independent in the performance of his/her functions. The Data Protection Commissionerôs function is to ensure that those who keep personal data in respect of individuals comply with the provisions of the Data Protection Acts.

The Commissioner maintains a register, available for public inspection, giving general details about the data handling practices of a range of data controllers, such as Government Departments, state agencies and financial institutions.

The Data Protection Commissioner has a wide range of enforcement powers to assist in ensuring that the principles of Data Protection are being observed. These include the serving of legal notices compelling a data controller to provide information needed to assist his enquiries, compelling a data controller to implement a provision in the Act, etc.

The Data Protection Commissioner also investigates complaints made by the general public in relation to personal data and has wide powers in this area. For example, the Commissioner may authorise officers to enter premises and to inspect personal information held on computer or relevant paper filing system. Members of the public who wish to make formal complaints may do so by writing to the Office of the Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois, or by email to info@dataprotection.ie.

Where employees of the organisation, in the normal course of their duties, become aware that an individual including employees of the organisation may be breaching the Acts or have committed or are committing an offence under the Acts, they should report the matter to **[INSERT NAME AND CONTACT DETAILS OF CEO AND VEC]**. A data controller found guilty of an offence under the Acts can be fined amounts up to ú100,000 on conviction and/or may be ordered to delete all or part of a database if relevant to the offence.

Advice/Assistance
All requests for advice and assistance on data protection issues within the VEC should be directed to **[INSERT APPROPRIATE CONTACT INFORMATION HERE]**.

Applying for Access to Personal Data
Requests for personal data should be made in writing to: **[The CEO, INSERT APPROPRIATE VEC CONTACT INFORMATION HERE]**.

Responding to Requests
When a valid request is received, the VEC must reply within 40 days[3], even if personal data is not held.

[3] 21 days if the request is to be informed if any personal data is held and to be given a description of the data and the purposes for which they are kept (Section 3 of the Data Protection Acts)

Useful Contacts
Data Protection Commissionerôs Office,
Phone: 1890 252231

http://www.dataprotection.ie
info@dataprotection.ie

Appendix 3

Protecting the confidentiality of Personal Data
Guidance Note

CMOD
Department of Finance
December 2008

Contents

Introduction

Under the Data Protection Acts, 1988 and 2003, Government Departments, Offices and Agencies, as data controllers, have a legal responsibility to:-

- obtain and process personal data fairly;
- keep it only for one or more specified and explicit lawful purposes;
- process it only in ways compatible with the purposes for which it was given initially;
- keep personal data safe and secure;
- keep data accurate, complete and up-to-date;
- ensure that it is adequate, relevant and not excessive;
- retain it no longer than is necessary for the specified purpose or purposes; and,
- provide a copy of his/her personal data to any individual, on request.

The purpose of these guidelines is to assist Departments, Offices and Agencies in implementing systems and procedures that will ensure, as much as possible, that personal data in their possession is kept safe and secure and to help Departments,
Offices and Agencies meet their legal responsibilities as set out above. This document can be expanded upon by Departments[4] to create detailed policies and procedures which reflect their specific business requirements.

Any queries in relation to the content of this document should be forwarded via email to dpguidelines@finance.gov.ie

Scope

This document provides guidelines on how personal data is to be stored, handled and protected under the following headings:-

a. General Procedures;
b. Paper Records;
c. Email and Personal Productivity Software;
d. Electronic Remote Access;
e. Laptops/Notebooks;
f. Mobile Storage Devices;
g. Data Transfers;
h. Inappropriate Access/Audit Trail Monitoring;
i. Breach Management.

Audience

The information contained in this document is intended for general distribution. However, it is especially important that senior management in Departments are aware of the contents of the document as the responsibility rests with them to ensure that the guidelines contained in it are followed. The guidelines should also be brought to the attention of all staff whose work involves the handling of personal data.

[4] For ñDepartmentsòread ñDepartments, Offices and Agenciesòthroughout this document

General Procedures

This document sets out guidelines in a number of specific areas where particular attention should be paid in order to help protect the confidentiality of personal data held in a Department. There are, however, a number of general procedures which Departments should follow:-

1. The first stage in establishing policies and procedures to ensure the protection of personal data is to know what data is held, where it is held and what the consequences would be should that data be lost or stolen. With that in mind, as a first step Departments should conduct an audit identifying the types of personal data held within the organisation, identifying and listing all information repositories holding personal data and their location. Risks associated with the storage, handling and protection of this data should be included in the Departmentôs risk register. Departments can then establish whether the security measures in place are appropriate and proportionate to the data being held while also taking on board the guidelines available in this document;

2. Access to all data centres and server rooms used to host hardware and software on which personal data is stored should be restricted only to those staff members that have clearance to work there. This should, where possible, entail swipe card and/or PIN technology to the room(s) in question ï such a system should record when, where and by whom the room was accessed. These access records and procedures should be reviewed by management regularly;

3. Access to systems which are no longer in active use and which contain personal data should be removed where such access is no longer necessary or cannot be justified;

4. Passwords used to access PCs, applications, databases, etc. should be of sufficient strength to deter password cracking or guessing attacks. A password should include numbers, symbols, upper and lowercase letters. If possible, password length should be around 12 to 14 characters but at the very minimum 8 characters. Passwords based on repetition, dictionary words, letter or number sequences, usernames, or biographical information like names or dates must be avoided. Departments must also ensure that passwords are changed on a regular basis;

5. Departments should have procedures in place to properly evaluate requests from other organisations for access to personal data in its possession. Such procedures should assist Departments in assessing whether the release of personal data is fully justifiable under the Data Protection Acts. Departments should also ensure that access by staff of personal data for analysis or research purposes is fully justifiable and proportionate;

6. Personnel who retire, transfer from the Department, resign etc. should be removed immediately from mailing lists and access control lists. Relevant changes should also occur when staff are transferred to other assignments internally. It is the responsibility of Departments to ensure that procedures are in place to support this, i.e. so that notification is provided to the relevant individual(s)/Unit in a timely fashion;

7. Contractors, consultants and external service providers employed by Departments should be subject to strict procedures with regard to accessing personal data by way of formal contract in line with the provisions of the Data Protection Acts. The terms of the contract and undertakings given should be subject to review and audit to ensure compliance;

8. Departments should have in place an up-to-date Acceptable Usage Policy in relation to the use of Information and Communications Technology (e.g. telephone, mobile phone, fax, email, internet, intranet and remote access, etc.) by its staff. This policy should be understood and signed by each user of such technology in the Department;

9. Departmentsô Audit Committees, when determining in consultation with Secretaries General (or CEOs, etc. where relevant) the work programme of their Internal Audit Units (IAUs), should ensure that the programme contains adequate coverage by IAUs of areas within their organisations which are responsible for the storage, handling and protection of personal data. The particular focus of any review by IAUs would be on assessing the adequacy of the control systems designed, in place and operated in these areas for the purpose of minimising the risk of any breach of data protection regulations. Risks associated with the storage, handling and protection of personal data should be included in the Departmentôs risk register and risk assessments should take place as part of a Departmentôs risk strategy exercise. Furthermore, external audits of all aspects of Data Protection within the organisation may be conducted on a periodic basis by the Office of the Data Protection Commissioner.

10. Procedures should be put in place in relation to disposal of files (both paper and electronic) containing personal data. In doing so, Departments should be aware of their legal obligations as set out in the National Archives Act, 1986 and the associated National Archives Regulations, 1988. It should be noted that incoming and outgoing emails which are ñof enduring interestô are archivable records under the Act. Procedures should also be put in place in relation to the secure disposal of computer equipment (especially storage media) at end-of-life. This could include the use of degaussers, erasers and physical destruction devices, etc;

11. Quality Customer Service documentation/customer charters should detail how customersô data is held and how it will be used/not used. Website privacy statements should be regularly reviewed to take account of any enhancements, new practices or additional services which involve the collection and use of personal data;

12. New staff should be carefully coached and trained before being allowed to access confidential or personal files;

13. Staff should ensure that callers to the office or other unauthorised persons are unable to view personal or sensitive information whether held on paper documents or information displayed on PC monitors, etc.;

14. All staff should ensure that PCs are logged off or ólockedô when left unattended for any period of time (e.g. in Windows, using Ctrl+Alt+Del keys). Where possible, staff should be restricted from saving files to the local disk. Users should be instructed to only save files to their allocated network drive;

15. Personal and sensitive information should be locked away when not in use or at end of day;

16. Appropriate filing procedures (both paper and electronic) should be drawn up and followed;

17. Departments should be careful in their use of the Personal Public Service Number (PPSN) in systems, on forms and documentation. There is a strict statutory basis providing for the

use of the PPSN. This allows organisations use the PPSN in support of a provision of a public service to a customer. The Department of Social & Family Affairs manages the issuance and use of PPS Numbers. A register of organisations that use the PPSN has been prepared and published to promote transparency regarding the ongoing use and future development of the PPSN as a unique identifier for public services. The register is available at: http://www.welfare.ie/EN/Topics/PPSN/Pages/rou.aspx .

18. Any databases or applications in use by Departments which contain personal data must be registered with the Office of the Data Protection Commissioner.

Paper Records

The Data Protection Acts apply equally to personal data held on ICT systems and on paper files. The following guidelines should be followed with regard to personal and sensitive data held on paper files:-

1. Paper records and files containing personal data should be handled in such a way as to restrict access only to those persons with business reasons to access them;
2. This should entail the operation of a policy whereby paper files containing such data are locked away when not required;
3. Consideration should also be given to logging access to paper files containing such data and information items;
4. Personal and sensitive information held on paper must be kept hidden from callers to offices;
5. Secure disposal of confidential waste should be in place and properly used. If third parties are employed to carry out such disposal, they must contractually agree to the Departmentôs data protection procedures and ensure that the confidentiality of all personal data is protected. Such contracts should contain clauses similar to those outlined in the section on ôData Transfersô below;
6. When paper files are transferred within a Department, this usually entails hand delivery. However, it should be noted that, in many cases, internal post in Departments ultimately feeds into the general postal system (this is particularly true for Departments with disparate locations). In these instances, senders must consider registered mail or guaranteed parcel post service where appropriate. Procedures must be in place for ensuring that the data is delivered only to the person to whom it is addressed, or another officer clearly acting on their behalf, and not any other staff member. Consideration should also be given to the security of manual files when in transit internally;
7. Facsimile technology (fax machines) should not be used for transmitting documents containing personal data.

Email and Personal Productivity Software

Email and other personal productivity software such as word processing applications, spreadsheets, etc. are valuable business tools which are in use across every Department. However, Departments must take extreme care in using this software where personal and sensitive data is concerned. In particular:-

1. Standard unencrypted email should **never** be used to transmit any data of a personal or sensitive nature. Departments that wish to use email to transfer such data must ensure that personal or sensitive information is encrypted either through file encryption or through the use of a s***ecure email*** facility which will encrypt the data (including any attachments) being sent. The strongest encryption methods available should be used. Departments should also

ensure that such email is sent only to the intended recipient. In order to ensure interoperability and to avoid significant key management costs, particular attention should be paid to any central solutions put in place for this purpose;
2. Departments should consider implementing solutions that scan outgoing emails and attachments for keywords that would indicate the presence of personal data and, if appropriate, prevent its transmission;
3. Where personal or sensitive data is held on applications and databases with relevant security and access controls in place, additional controls should be considered that would prevent such data from being copied to personal productivity software (such as word processing applications, spreadsheets, etc.) where no security or access controls are in place and/or can be bypassed.

Remote Access

There is an increasing business requirement for mobile working and e-working across the public service. Consequently, the demand from staff to access remotely the same systems that they can access from the office is increasing. This brings its own challenges in relation to data security which Departments must address. With regard to personal and sensitive data, the following guidelines should be adhered to:-

1. In the first instance, all personal and sensitive data held electronically should be stored centrally (e.g. in a data centre or in a Departmentôs secure server room with documented security in place). Data that is readily available via remote access should not be copied to client PCs or to portable storage devices, such as laptops, memory sticks, etc. that may be stolen or lost;
2. When accessing this data remotely, it must be done via a secure encrypted link (e.g. IPSEC or SSL VPN tunnel) with relevant access controls in place;
3. Additional stringent security and access controls should be in place, e.g. the mandatory use of strong passwords and security token authentication (i.e. twofactor authentication);
4. Data being accessed in this way should be prevented from being copied from the central location to the remote machine;
5. Departments must utilise technologies that will provide for the automatic deletion of temporary files which may be stored on remote machines by its operating system;
6. Departments should ensure that only known machines (whether desktop PC, laptop, mobile phone, PDA, etc.) configured appropriately to the Departmentôs standards (e.g. with up-to-date anti-virus and anti-spyware software, full encryption, etc.), are allowed to remotely access centrally held personal or sensitive data. The strongest encryption methods available should be used to encrypt data on these machines. In addition, óstrongô passwords/passphrases (see óGeneral Proceduresô) must be used to protect access to these machines and to encrypt/decrypt the data held on them;
7. Staff should be aware that it is imperative that any wireless technologies/networks used when accessing the Departmentôs systems should be encrypted to the strongest standard available.

Laptops and Other Mobile Storage Devices (incl. Mobile Phones, PDAs, USB memory sticks, External Hard Drives, etc.)

The use of laptops, USB memory sticks and other portable or removable storage has increased substantially in the last number of years. Likewise, the use of personal communications and storage devices such as mobile phones, PDAs, etc. has also increased. These devices are useful tools to

meet the business needs of staff. They are, however, highly susceptible to loss or theft. To protect the content held on these devices, the following recommendations should be followed:

1. All portable devices should be password-protected to prevent unauthorised use of the device and unauthorised access to information held on the device. In the case of mobile phones, both a PIN and login password should be used. Manufacturer or operator-provided PIN codes must be changed from the default setting by the user on receipt of the device;
2. Passwords used on these devices should be of sufficient strength to deter password cracking or guessing attacks. A password should include numbers, symbols, upper and lowercase letters. Password length should ideally be around 12 to 14 characters but at the very minimum 8 characters. Passwords based on repetition, dictionary words, letter or number sequences, usernames, or biographical information like names or dates must be avoided. Departments must ensure that passwords are regularly changed;
3. Personal, private, sensitive or confidential data should not be stored on portable devices. In cases where this is unavoidable, all devices containing this type of data must be encrypted. With regard to laptops, full disk encryption must be employed regardless of the type of data stored;
4. With regard to mobile technologies, staff should be aware that when óroamingô abroad, communications may not be as secure as they would be within Ireland;
5. Data held on portable devices should be backed up regularly to the Departmentôs servers;
6. When portable computing devices are being used in public places, care must be taken to avoid unwitting disclosure of information, e.g. through overlooking or overhearing by unauthorised persons;
7. Portable devices must not contain unauthorised, unlicensed or personally licensed software. All software must be authorised and procured through a Departmentôs IT Unit;
8. Anti-virus/Anti-spyware/Personal Firewall software must be installed and kept up to date on portable devices. These devices should be subjected to regular virus checks using this software;
9. Departments should ensure that when providing portable devices for use by staff members, each device is authorised for use by a specific named individual. The responsibility for the physical safeguarding of the device will then rest with that individual;
10. Laptops must be physically secured if left in the office overnight. When out of the office, the device should be kept secure at all times;
11. Portable devices should never be left in an unattended vehicle;
12. Portable storage media should only be used for data transfer where there is a business requirement to do so, should only be used on approved workstations and must be encrypted;
13. In order to minimise incidents of unauthorised access and/or incidents of lost/stolen data, Departments should restrict the use of personal storage media and devices (e.g. floppy disks, CDs, DVDs, USB memory sticks, etc.) to staff that require to use these media/devices for business purposes;
14. Only storage media provided by a Departmentôs IT Unit should be permitted for use with that Departmentôs computer equipment. Departments must put in place solutions which only allow officially sanctioned media to be used on a Departmentôs computer equipment (i.e. on networks, USB ports, etc.);
15. Staff owned devices such as portable media players (e.g. iPods, etc.), digital cameras, USB sticks, etc. must be technologically restricted from connecting to Department computers;
16. Departments should consider implementing additional log-in controls on portable devices such as laptops;
17. Departments should implement technologies that will allow the remote deletion of personal data from portable devices (such as mobile phones and PDAs) should such devices be lost

or stolen. A procedure for early notification of such loss should be put in place. This would allow for the disconnection of the missing device from a Departmentôs email, calendar and file systems;

18. Departments should implement procedures that will ensure that personal data held on mobile storage devices is fully deleted when the data is no longer required (e.g. through fully formatting the devicesô hard drive);

Data Transfers

Data Transfers are a daily business requirement for most, if not all, Government Departments. With regard to personal and sensitive data, such transfers should take place only where absolutely necessary, using the most secure channel available. To support this, Departments should adhere to the following:-

1. Data transfers should, where possible, only take place via secure on-line channels where the data is encrypted rather than copying to media for transportation. Where this is not possible or appropriate at present, the safety of the data should be ensured before, during and after transit;
2. Manual data transfers using removable physical media (e.g. memory sticks, CDs, tape, etc.) should end where possible;
3. In the meantime, where data is copied to removable media for transportation such data must be encrypted using the strongest possible encryption method available. Strong passwords/passphrases (see óGeneral Proceduresô) must be used to encrypt/decrypt the data;
4. Any such encrypted media should wherever possible be accompanied by a member of the Departmentôs staff, be delivered directly to, and be signed for by, the intended recipient. If this is not possible, the use of registered post or another certifiable delivery method may be used if an agreement similar to that outlined in 7. below has been put in place;
5. óStrongô passwords (see óGeneral Proceduresô) must be used to protect any encrypted data. Such passwords must not be sent with the data it is intended to protect. Care should be taken to ensure that the password is sent securely to the intended recipient and that it is not disclosed to any other person;
6. Standard email should never be used to transmit any data of a personal or sensitive nature. Departments that wish to use email to transfer such data must ensure that personal or sensitive information is encrypted either through file encryption or through the use of a ***secure email*** facility which will encrypt the data (including any attachments) being sent. Staff should ensure that such mail is sent only to the intended recipient. In order to ensure interoperability and to avoid significant key management costs, particular attention should be paid to any central solutions put in place for this purpose;
7. When a data transfer with a third party is required (including to/from other Government Departments), a written agreement should be put in place between both parties in advance of any data transfer. Such an agreement should define:-
    - The information that is required by the third party (the purposes for which the information can be used should also be defined if the recipient party is carrying out processing on behalf of the organisation);
    - Named contacts in each organisation responsible for the data;
    - The frequency of the proposed transfers;
    - An explanation of the requirement for the information/data transfer;
    - The transfer method that will be used (e.g. Secure FTP, Secure email, etc.);
    - The encryption method that will be used;
    - The acknowledgement procedures on receipt of the data;

- The length of time the information will be retained by the third party;
- Confirmation from the third party that the information will be handled to the same level of controls that the Department apply to that category of information;
- Confirmation as to the point at which the third party will take over responsibility for protecting the data (e.g. on confirmed receipt of the data);
- The method of secure disposal of the transfer media and the timeline for disposal;
- The method for highlighting breaches in the transfer process;
- For data controller to data controller transfers (as opposed to a data controller to a data processor transfer), it needs to be clear that only necessary data is transferred to meet the purposes;
- Business procedures need to be in place to ensure that all such transfers are legal, justifiable and that only necessary data is transferred to meet the purposes;
- Particular attention should be focussed on data made available to third party data processors under contract for testing purposes. Live data should not be used for this purpose.

Appropriate Access and Audit Trail Monitoring

All organisations have an obligation to keep information ósafe and secureô and have appropriate measures in place to prevent ñunauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destructionò in compliance with sections 2(1)(d) and 2C of the Data Protection Acts 1988 & 2003.

It is imperative, therefore, that Departments have security in place to ensure that only those staff members with a business need to access a particular set of personal or sensitive data are allowed to access that data. In addition to this general requirement, the following guidelines should be followed:-

1. Departments should ensure that their ICT systems are protected by use of appropriate firewall technologies and that this technology is kept up-to-date and is sufficient to meet emerging threats;
2. In order to capture instances of inappropriate access (whether internal or external), addition, deletion and editing of data, audit trails should be used where technically possible. In situations where systems containing personal data do not currently record óviewô or óreadô access, it should be investigated, as a matter of urgency whether such functionality can be enabled. In carrying out such an investigation, Departments should take into account whether there would be any effect on system performance that may hinder the ability of the Department to conduct its business. If the functionality cannot be enabled and the risk of inappropriate access is sufficiently high, such systems should be scheduled for removal from use and replaced by systems with appropriate auditing functionality;
3. Access to files containing personal data should be monitored by supervisors on an ongoing basis. Staff should be made aware that this is being done. IT systems may need to be put in place to support this supervision.

Breach Management

A data security breach can happen for a number of reasons, including:-

- Loss or theft of data or equipment on which data is stored (including break-in to an organisationôs premises);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;

- Human error;
- Unforeseen circumstances such as a flood or fire;
- A hacking attack;
- Access where information is obtained by deceiving the organisation that holds it.

It is important that Departments put into place a breach management plan to follow should such an incident occur. There are five elements to any breach management plan:-

1. Identification and Classification
2. Containment and Recovery
3. Risk Assessment
4. Notification of Breach
5. Evaluation and Response

1. Identification and Classification

Departments must put in place procedures that will allow any staff member to report an information security incident. It is important that all staff are aware to whom they should report such an incident. Having such a procedure in place will allow for early recognition of the incident so that it can be dealt with in the most appropriate manner. Details of the incident should be recorded accurately, including the date and time the incident occurred, the date and time it was detected, who/what reported the incident, description of the incident, details of any ICT systems involved, corroborating material such as error messages, log files, etc. In this respect, staff need to be made fully aware as to what constitutes a breach.

2. Containment and Recovery

Containment involves limiting the scope and impact of the breach of data protection procedures. If a breach occurs, Departments should:-

- decide on who would take the lead in investigating the breach and ensure that the appropriate resources are made available for the investigation;
- establish who in the organisation needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. For example, this might entail isolating a compromised section of the network, finding a lost file or piece of equipment, or simply changing access codes to server rooms, etc.;
- establish whether there is anything that can be done to recover losses and limit the damage the breach can cause;
- where appropriate, inform the Garda.

3. Risk Assessment

In assessing the risk arising from a data security breach, Departments should consider what would be the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences will materialise and, in the event of materialising, how serious or substantial are they likely to be. In assessing the risk, Departments should consider the following points:-

- what type of data is involved?;
- how sensitive is it?;
- are there any protections in place (e.g. encryption)?;
- what could the data tell a third party about the individual?;
- how many individualsôpersonal data are affected by the breach?;

4. Notification of Breaches

Although there is no current explicit legal obligation to notify individuals or other bodies under the Data Protection Acts of a breach, the Data Protection Commissionerôs Office encourages voluntary notification and early engagement with the Office. Therefore, if inappropriate release/loss of personal data occurs it should be reported immediately, both internally and to the Data Protection Commissionerôs Office and, if appropriate in the circumstances, to the persons whose data it is. In this regard, Departments should be aware of the dangers of óover notifyingô. Not every incident will warrant notification. For example, notifying a whole 200,000 strong customer base of an issue affecting only 2,000 customers may cause disproportionate enquiries and work.

When notifying individuals, Departments should consider using the most appropriate medium to do so. They should also bear in mind the security of the medium used for notifying individuals of a breach of data protection procedures and the urgency of the situation. Specific and clear advice should be given to individuals on the steps they can take to protect themselves and what the Department is willing to do to assist them.

Departments should also provide a way in which individuals can make contact for further information, e.g. a helpline number, webpage, etc.

Departments should consider notifying third parties such as the Garda, bank or credit card companies who can assist in reducing the risk of financial loss to individuals.

The Office of the Data Protection Commissioner will provide advice upon notification as to the requirement or otherwise, in particular circumstances, to notify individuals.

5. Evaluation and Response

Subsequent to any information security breach a thorough review of the incident should occur. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved. Any recommended changed to policies and/or procedures should be documented and implemented as soon as possible thereafter.

Each Department should identify a group of people within the organisation who will be responsible for reacting to reported breaches of security.

Appendix 4

***Template* Breach Management Policy**

<Name of VEC>

Policy

Safeguarding personally identifiable information in the possession of ***<name of Vocational Education Committee>*** (the VEC) and preventing its breach, is essential to ensure The VEC retains the trust of both staff and the public. The VEC has in place a Data Breach Notification Policy/Plan including procedures that address both the protection of certain information, including ñPersonal Informationò as defined in the Data Protection Act 1988 and Amendment Act 2003, and the prompt notification of those individuals actually or potentially affected by a breach of the security of the systems used by the VEC.

For the purpose of this policy the term **"breach"** includes the loss of control, compromise, unauthorised disclosure or unauthorised access or potential access to personally identifiable information, whether in physical (paper) or electronic form.

The VEC will make all reasonable efforts to protect confidential information and specifically non-public personal information as a ñData Controllerò when it acts in that capacity.

The VEC will make all reasonable efforts to protect such information under the VECôs control from unauthorised access, use, disclosure, deletion, destruction, damage or removal. Although reasonable efforts are made to protect facilities, equipment, resources and data, there exists the possibility that the security of data maintained by the VEC may be breached. As a result, this policy requires that the VEC has a reasonable and appropriate breach notification procedure or action plan in place should security procedures not prevent a breach. ***(VEC Breach Notification Plan).***

This policy should be read in conjunction with the Data Protection Commissioner's Personal Data Security Breach Code of Practice and the Code of Practice for the Protection of Personal Data in VECs.

Purpose

The purpose of this policy is to acknowledge the importance of information security and to recognise that a breach may still occur and therefore to establish a framework for addressing a breach that occurs.

Scope

This policy applies to all personnel, schools/colleges and other education and administrative centres under the remit of the VEC.

1.0 Responsibility

VEC staff are responsible for ensuring that appropriate and adequate protection and controls are in place and applied in each facility and resource under their control and identifying

those that are not. CEO, APO, Principals, Centre Managers and Heads of Department are responsible for ensuring that staff follow the intent of this Policy and are adhering to all related procedures.

Periodic reviews of the measures and practices in place should be carried out.

2.0 Data Security[5]

High standards of physical and technical security are essential to protect the confidentiality of personal data. These include:

- ensuring access to information is restricted to authorised staff in accordance with defined policy
- ensuring computer systems are password protected
- keeping information on computer screens and paper files hidden from callers to offices[6]
- ensuring that no documentation of a ñconfidential/sensitive natureò is left on desks/photocopiers etc.
- ensuring that personal data is protected by strong encryption when being stored on portable devices or transferred electronically (including email)
- ensuring that personal data is not stored on portable devices except in essential circumstances. Where deemed essential, the data must be encrypted and a record kept of the nature and extent of the data and why it is being stored on a portable device. Arrangements should be put in place to fully delete the data on the portable device when it is no longer being used
- having appropriate facilities in place for disposal of confidential waste
- non-disclosure of personal security passwords to any other individual (including other employees within the organisation)
- keeping premises secure, especially when unoccupied
- keeping audit logs in relation to read access, changes, additions deletions on ICT system
- having adequate security measures and policies in place in relation to the use of laptops and other mobile storage devices
- inserting appropriate data protection and confidentiality clauses in arrangements with any processors of personal data on the organisationôs behalf, including:
  - the conditions under which data may be processed
  - the minimum security measures that the data processors must have in place
  - mechanisms or provisions that will enable the data controller to ensure that any data processor is compliant with the security practices which include a right of inspector or independent audit

3.0 Breach Incident Handling and Reporting Requirements

When faced with a breach of security incident the VEC must be able to respond in an appropriate manner protecting both its own information and helping to protect the information of others who might be affected by the incident. The VECôs Data Breach Notification Policy/Plan outlines the roles and responsibilities of relevant personnel, in the prevention of security breaches and in dealing with threats of breaches or actual breaches and responding by implementing the appropriate recovery and reporting procedures.

[5] This section should be read in conjunction with the ICT Acceptable Use Policy.

4.0 Data Breach Notification Policy/Plan

It is necessary for the VEC, in the course of its business, to collect and use data (information in a form which can be processed) for a variety of purposes, about its staff, students and other individuals with whom they come in contact.

Due to the increasing frequency of information security breaches it is important that staff understand the repercussions a data security breach can have on the VEC ï from the moment the breach is detected to the way we respond after the breach occurs.

A data security breach can happen for a number of reasons, including:-

- loss or theft of data or equipment on which data is stored (including break-in to any of our premises)
- inappropriate access controls allowing unauthorised use
- equipment failure
- human error
- unforeseen circumstances such as flood or fire
- a hacking attack
- access where information is obtained by deceiving the organisation that holds it.

The VEC has adopted the following plan for use in the event of data breaches:

(i) Identification and Classification

Staff must be made fully aware as to what constitutes a breach, how it may occur, who to contact when one happens and how to log the details.

A Breach Management Team (BMT) must be established with representatives from each School/Centre/Office within the VEC, as well as a team leader with decision making authority. The team will evaluate all breaches, their impact and formulate a plan on how to proceed. Each team member will have a backup member to cover holidays, sick leave etc.

(ii) Containment & Recovery

Containment involves limiting the scope and impact of the breach of data protection procedures.

The Breach Management Team will evaluate the breach; determine what damage may be caused, and then try to limit the damage and impact caused by the breach. The team will make recommendations to ensure such an incident cannot happen again.

The Breach Management Team leader will be responsible for ensuring that the required resources are in place to investigate the breach and will take the lead in the investigation. If specialist resources (IT, Legal, Financial etc) are required the BMT leader will get them involved as soon as possible.

Relevant the VEC staff will be notified of the breach and how they are to help in the investigation.

The Breach Management Team will decide whether to notify data subjects and if so this should be done without delay.

Should a serious breach take place the team leader will contact the Gardaí and Data Protection Commissioner and act as liaison with them.

(iii) Incident Response DOs and DON'Ts for IT systems

DO'S

- immediately isolate the affected system to prevent further intrusion, release of data, damage etc.
- use the telephone to communicate. Attacker may be capable of monitoring e-mail traffic
- preserve all pertinent logs, e.g. firewall, router and intrusion detection system.
- make back-up copies of damaged or altered files and keep these backups in a secure location.
- identify where the affected system resides within the network topology
- identify all systems and agencies that connect to the affected system
- identify the programs and processes that operate on the affected system(s), the impact of the disruption and the maximum allowable outage time.
- in the event the affected system is collected as evidence, make arrangements to provide for the continuity of services i.e. prepare redundant system and obtain data back-ups.

DON'Ts

- delete, move or alter files on the affected systems
- contact the suspected perpetrator
- conduct a forensic analysis

(iv) Risk Assessment

Assessing the risk will depend on how likely it is that adverse consequences will materialise, and in the event of materialising, how serious or substantial they are likely to be. The following needs to be considered:

1. the type of data involved e.g. personal, financial or medical
2. how long the breach has been going on. How sensitive the data is? Some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)
3. if data has been lost or stolen, was encryption or other protection methods in place?

4. what has happened to the data? If data has been stolen it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been altered or damaged, this poses a different type and level of risk
5. how many individuals are affected?
6. what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic thief while the loss of apparently trivial piece of information could help a fraudster build up a detailed picture for identity theft
7. who are the individuals whose data has been breached?
8. what harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these as well as other aspects of their life?
9. are there wider consequences to consider such as loss of public confidence in the service we provide?
10. if information has been deleted can it be retrieved from backup systems?

(v) Notification of a Breach

As soon as personal data for which you are responsible has been compromised ï e.g. through loss of a portable device, misaddressing of labels, sensitive information left where unauthorised viewing could take place ï i.e. photocopies not properly disposed off or left on copier, you should complete the Data Security Breach Incident Report and immediately notify your Principal/Manager/Director who will investigate the issues surrounding the breach. The seriousness of the breach will determine the type of investigation that will take place. It may include an on-site examination of systems and procedures. In the event of a serious data security breach the Breach Management Team will be informed and contact will be made with the Office of the Data Protection Commissioner for advice and clarification.

Where appropriate the Breach Management Team will put a communication plan in place to contact the owner of the data involved (the data subject). Security of the medium used for notifying individuals of a breach of data protection procedures and urgency of situation should be borne in mind. Specific and clear advice should be given to individuals on the steps they can take to protect themselves and what the VEC is willing to do to assist them. Provision of a helpline number or a web page should be considered. Notifications may be delayed if the Gardaí advise that it will impede an investigation.

(vi) Media

Media enquiries about the breach should be dealt with by authorised personnel only. A centralised ñFact Sheetò should also be created to ensure that one version, not many, becomes the view of the organisation internally and in contacts with the media.

The VEC should consider notifying third parties such as the Gardaí, bank or credit card companies who can assist in reducing the risk of financial loss to individuals.

(vii) Evaluation and Response

Subsequent to any information security breach a thorough review of the incident should occur. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

Any recommended changes to policies and/or procedures should be documented and implemented as soon as possible thereafter.

The plan will also be reviewed periodically as new issues and technologies may arise which will have a bearing on the way it is implemented.

5.0 Breach Management Team

NAME	LOCATION	CONTACT NUMBER
	CEO / APO	
	Finance	
	Human Resources	
	Education Support Services	
	School/Centre/Office	

Data Protection Commissioner
Office of the Data Protection Commissioner
Canal House, Station Road, Portarlington, Co.Laois
Tel: 1890 252 231
E-mail: info@dataprotection.ie
Web: www.dataprotection.ie

References: Data Protection Act 1988 and (Amendment) Act 2003

Data Protection Commissionerôs Personal Data Security Breach Code of Practice

The VEC Data Protection Policy

The VEC ICT Acceptable Usage Policy

The VEC CCTV Policy

Code of Practice for the Protection of Personal Data in VECs.

Data Security Breach – Incident Report

Breach ID:

When did the breach take place?

When was the breach discovered?

Who reported the breach?

Were there any witnesses? If Yes, state Names.

Please provide details of the breach:

Were any IT systems involved? If so please list them.

Is any additional material available e.g. error messages, screen shots, log files, CCTV?

Any additional comments?

Signed:_____

Date: _____ **Time:** _____

For Breach Management Team Use

Details logged by _____

Severity of the breach (0 being minor, 5 being critical)

0 1 2 3 4 5

Data Subjects to be notified Yes ☐ No ☐

Details:_____
_____

Data Protection Commissioner to be notified Yes ☐ No ☐

Details (Date/time, note of advice received):_____
_____

Gardaí to be notified Yes ☐ No ☐

Details:_____
_____