etb
Bord Oideachais agus Oiliúna
Átha Cliath agus Dhún Laoghaire
Dublin and Dún Laoghaire
Education and Training Board

DDLETB Compliance Checklist

Date: July 2017

Objective: To create awareness around the responsibilities for schools/centres with respect to Data Protection principles and the obtaining and use of personal data in a school/centre context.

Purpose: To allow school/centre management to carry out a quick check on data protection compliance.

How to use this checklist:

Step One: Familiarise yourself with these Guidelines, particularly What is Data Protection and why is it important for schools/centres.

Step Two: Having familiarised yourself with the Data Protection Guidelines, you should now answer the questions to inform yourself with respect to your own school's/centres needs and the drafting of your own school/centre Data Protection Policy. **Note to ETB Schools/Centres**: ETB Schools/centres should each have a Data Protection Policy in place. The Policy should be that promulgated by the ETB Committee and distributed to the School Board of Management to be ratified and adopted by the ETB school/centre. In this way, each ETB School/centre in an ETB area will have a consistent Data Protection Policy.

Step Three: Develop your school's/centres Data Protection Policy having completed Step One and Step Two above.

Introduction

School/centre management bodies (primary and post-primary) have prepared this checklist to assist school/centre management review how it handles personal data. It should be of particular help to a school/centre carrying out an audit of its compliance with the Data Protection Acts and specifically a school/centre preparing and devising its Data Protection Policy.

The Data Protection Acts impose the following obligations on all organisations that handle personal data[1]:

1. Obtain and process information fairly

[1] Personal data means any information that can be linked to a living individual. The definition is deliberately broad.

2. Keep it only for one or more specified, explicit, and lawful purpose(s)
3. Use and disclose it only in ways compatible with the purposes for which it was initially given
4. Keep it safe and secure
5. Keep it accurate, complete, and up-to-date
6. Ensure that it is adequate, relevant, and not excessive
7. Retain it for no longer than is necessary for the purpose or purposes for which it was initially given
8. Give a copy of his/her personal data to an individual, on request.

It is important that a school/centre has procedures in place to ensure that it is compliant with these obligations in relation to all categories of personal data that it handles. DDLETB's Data Protection Policy and supporting procedures should therefore always be documented.

1. Inventory of Personal Data Holdings:

For the purposes of the inventory, have you conducted an audit of the various categories of personal data holdings in your school/centre?	Yes	No
For additional information see Important Terms in Data Protection and Sensitive Personal Data before answering this question.		

Who holds the responsibility for the control of the data? Example: Staff records held by ……. Payroll details held by…………	
Is there a system for classifying information (e.g. sensitive, confidential) with corresponding levels of access to such information?	

2. Personal Data held by Schools/Centres:

Definitions: **Personal data** is 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. This can be a very wide definition, depending on the circumstances. **Sensitive personal data** relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence, any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings; trade union membership.

Classes of individuals about whom the school/centre holds personal data include the following:
Staff
Students

Traninees
Parents

How do you obtain personal data? *Example: Enrolment Form, CV/Application Form*		
What types of personal data do you obtain? *Example: Date of Birth, Mother's Maiden Name*		
Do you record the Personal Public Service Number - PPSN? *Example: Payroll* *Primary Level: Limited obligation, example Resource* *Post-Primary: Obligation, example, student personal identifier/October Returns*		
Do you explain to individuals why you are collecting particular items of personal data and the purpose for which you are going to use it (when this is not obvious)?	**Yes**	**No**
Is verification documentation sought? If so, what happens to verification documentation? Is a copy made and retained for your records? *Example: Garda Vetting, Teacher Registration*		
What procedures are in place to ensure that a person's data is being recorded accurately?		
Have you established the retention period for the personal data retained both in computer and manual form? For guidance, see the Records Retention Schedule.	**Yes**	**No**
Action Item:		
Are records stored in a secure location? For guidance, see Storage & Security of Personal Data		

3. School/Centre Employees' Personal Data:

(Refer to Guidance on school records and retention periods

How do you obtain personal data?	
What types of personal data do you obtain?	
Do you explain to employees why you are collecting particular items of personal data and the purpose for which you are going to use it (when this is not obvious)?	
Is verification documentation sought? If so, what happens to verification documentation?	
What do you do with approved and rejected application forms?	
Are all details received input onto a computer system?	
What procedures are in place to ensure that a person's data is being recorded accurately?	
For how long is personal data retained both in computer and manual form?	
How long are personnel files (computer and manual) held after the staff member has left employment?	
Is any employee monitoring taking place re usage of email and internet etc? If so, what information is provided to employees? Is there a policy in place setting out the terms of such monitoring and has it been brought to the attention of all staff?	

Are records stored in a secure location?	

4. Employee Sensitive Personal Data:

(Refer to Important Terms in Data Protection and Sensitive Personal Data

Do you process any sensitive personal data[2]?	
Under what circumstances do you obtain sensitive data?	
Who has access to sensitive data?	
What constitutes a need to access medical data?	
Who determines which staff may gain access to the data?	
Is sensitive personal data transmitted internally/externally? *Example: Vetting; Medmark*	
In the case of sensitive personal data, have you sought explicit consent from the individual for the holding and or disclosure of such data?	
How is the data transmitted? Encrypted email? Secure fax?	
For how long is sensitive personal data retained in both computer and manual form?	

[2] "Sensitive Personal Data" is defined in the Data Protection Acts as personal data relating to: racial or ethnic origin; political opinions or religious or philosophical beliefs; membership of a trade union; physical or mental health or condition or sexual life; commission or alleged commission of an offence and proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

5. The School's/Centres Student Records

(Refer to Guidance on school records and retention periods and Records Retention Schedule

How do you obtain personal data?	
What types of personal data do you obtain?	
Do you explain to parents/students why you are collecting particular items of personal data and the purpose for which you are going to use it (when this is not obvious)?	
Is verification documentation sought? If so, what happens to verification documentation?	
What specified purpose do you hold these student records for?	
Are all details received input onto a computer system?	
What procedures are in place to ensure that a student's data is being recorded accurately?	
For how long is personal data retained both in computer and manual form?	
How long are student files (computer and manual) held after the student has left the school/centre?	
Are records stored in a secure location?	

6. Student Sensitive Personal Data:

(Refer to Important Terms in Data Protection and Sensitive personal Data

Do you process any sensitive personal data[3]?	
Under what circumstances do you obtain sensitive data?	
Who has access to sensitive data?	
What constitutes a need to access "medical data"/"social work data"?	
Who determines which staff may gain access to the data?	
Is sensitive personal data transmitted internally/externally? *Example: HSE, DES, NCSE, SENO, NEWB etc.*	
In the case of sensitive personal data have you sought explicit consent from the individual parent/guardian/student for the holding and/or disclosure of such data?	
How is the data transmitted? Encrypted email? Secure fax?	
For how long is sensitive personal data retained in both computer and manual form?	

[3] "Sensitive Personal Data" is defined in the Data Protection Acts as personal data relating to: racial or ethnic origin; political opinions or religious or philosophical beliefs; membership of a trade union; physical or mental health or condition or sexual life; commission or alleged commission of an offence and proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

7. ETB/Board of Management

(Refer to Guidance on school records and retention periods)

How do you obtain personal data on board of management members?	
What types of personal data do you obtain?	
For what purpose do you keep records for the appointment/nomination to the board?	
Do you explain to board members why you are collecting particular items of personal data and the purpose for which you are going to use it (when this is not obvious)?	
Are all details received input onto a computer system?	
What procedures are in place to ensure that a person's data is being recorded accurately?	
For how long is personal data retained both in computer and manual form?	
How long are board members' details (computer and manual) held after they cease to be members of the board?	
How are minutes of meetings and correspondence which may include references to particular individuals recorded?	
Are records stored in a secure location?	
Is sensitive documentation circulated for discussion at board of management meetings (e.g. child protection reports concerning employees) only circulated in hard copy at the beginning of such meetings and gathered up at the end to be stored in the DLP's secure storage facility?	

At the end of a board of management term, are all documents relating to board of management business gathered up from members to be safely and securely destroyed?	

8. Requests for Access, Correction, Deletion:

Refer to: Guidance on requests for access to information held and rectifying personal data held and the following forms: Data Access Request Form and see the Personal Data Rectification Erasure Form

How do you handle access requests received under the DP Acts?	
Are you clear as to what information you are obliged to release?	
Are you clear as to what information you are, in certain circumstances, prohibited from releasing (e.g. health data, social work data)?	
Do you ensure that all third party data is redacted before releasing the materials to a data subject?	
Are you clear as to what information you are, in certain circumstances, entitled to withhold from an access request?	
Where you withhold information from an access request, do you inform the data subjects of the reasons for this and advise them of their right to complain to the Office of the Data Protection Commissioner?	
Are employees / students /trainees / parents / guardians familiar with the process relating to making an access request?	

Are you in a position to respond to such a request within the statutory 21 or 40 day periods[4]? Does the response include reference to the right to complain to the Office of the Data Protection Commissioner?	
How do you check personal data for accuracy?	
Do you know how much of the personal data you hold is time-sensitive (i.e. likely to become inaccurate over time unless it is updated)?	
Do you take steps to ensure your databases are kept up-to-date?	
What procedures are in place to amend or delete inaccurate or unnecessary data within 40 days of being notified of same?	

9. Transfers to Third Parties:

*(*Refer to Third party service agreements and Transferring personal data abroad

Do you transfer/disclose personal data to third parties, either on your own initiative or on request?	
Where the transfers are to Government Departments, are the transfers in compliance with the "Protection of the Confidentiality of Personal Data Guidance Notes" issued by the CMOD, Department of Finance, December 2008?	
Are there procedural guidelines to deal with requests for personal data from third parties?	

[4] 21 days to provide a description of the personal data and the purposes for which they are kept (where the request is made under section 3 of the Data Protection Acts); 40 days to provide a copy of the data (i.e. a request made under section 4 of the Data Protection Acts).

Do these guidelines reflect careful consideration of the legal basis in the Data Protection Acts[5] for the provision of such information to third parties?	
Do you inform employees / students / parents / guardians of such disclosures?	
Do you document all requests received and responses made?	
Where you transfer personal data to third parties to be processed by them (e.g. CCTV system operators, HR/payroll companies, cloud computing, archiving services etc.), do you have a service-level agreement/data processing agreement in place?	
Does the data processing agreement/service-level agreement comply with data protection law? See Third party service agreements	
Has the school's/centres Personal Data Security Breach Code of Practice been incorporated into the data processing agreement/service-level agreement in place with third party data processors? See Third party service agreements	

[5] The default enabler under the Acts is the freely-given, informed consent of the individual data subject. Another enabler would be where there is a legal obligation to provide the information (for example, payroll information to the Revenue Commissioners). In other cases the law may permit, but not require, the disclosure of personal data - for example, to the Garda Síochána or to the Department of Social Protection for anti-fraud purposes. In such cases, the organisation must make its own assessment of what personal data it would be justified in providing on a case-by-case basis. For further guidance and assistance, see State Institution Requests

.

10. Retention and Disposal:

Refer to: Storage & Security of Personal Data and Guidance on school records and retention periods

Is there a clear policy on how long items of information are to be retained, taking account of legal requirements[6]?	
Do you purge your databases of data which you no longer need in a regular, safe and secure manner?	
Do you have a policy on the safe and secure disposal/deletion of personal data as soon as the purpose for which you obtained the data has been completed?	
Are the systems for the disposal of personal data secure?	

11. CCTV:

Refer to link*:* Use of CCTV systems in schools See also CCTV Policy Template

Is CCTV in operation?	
If yes, are you aware of its possible limited usage?	
If no, but it is intended that a CCTV system be installed in the school/centre, has a Privacy Impact Assessment been carried out (see the Appendix to the template CCTV policy) and have the staff, school/centre community, students, parents etc. been consulted?	

[6] e.g. Revenue Commissioners, authorisation from the Director of the National Archives.

Do you have a policy with regard to the operation of CCTV?	
What is the retention period for CCTV footage?	
Are equipment and tapes/discs stored securely?	
Who has access to CCTV images?	
Is CCTV used for reasons other than security?	
Is there appropriate signage in relation to CCTV?	
Have you ensured that the location and positioning of CCTV cameras complies with guidance issued by the Office of the Data Protection Commissioner? See Use of CCTV systems in schools and Guidelines issued by the Data Protection Commissioner	
Are employees / students / parents / guardians / visitors aware of the purpose of CCTV?	
Are you in a position to comply with data access requests for images/recordings made by the CCTV system?	
If the CCTV is monitored/run by a third party (external security company), do you have a written data processing agreement in place with them? See Third party service agreements	

12. Direct Marketing:

Refer to link: Schools and Direct Marketing

Are you aware of your obligations with respect to direct marketing?	

13. Contracts with Data Processors:

Refer to links: Third party service agreements

Do you outsource any processing of personal data?	
How are individuals made aware that their personal data may be outsourced to a third party?	
Do you have written contracts in place with such data processors which comply with the Data Protection Acts? See Third party service agreements	
Has the school's/centres Personal Data Security Breach Code of Practice been incorporated into any data processing agreement/service-level agreement reached with data processors?	

14. The School's Computer System & Security:

Refer to links: Storage & Security of Personal Data and also Third party service agreements

Does your school/centre have computer usage guidelines (including internet and email usage, e.g. IT Acceptable Usage Policy) in place and are they up-to-date? Have the guidelines been brought to the attention of all staff members and are refresher training sessions given regularly?	
Are passwords (or other forms of authentication) in use?	
How often are passwords changed?	
Who can change a password?	

Are there access-level restrictions?	
Who assigns access levels?	
If documents containing personal data are sent externally by email, are they encrypted or password protected?	
Is there a clear procedure governing the granting and removal of access for employees/students on enrolling and leaving the school/centre?	

Removable Media:

Are ports such as CD/USB drives enabled? Are such drives capable of copying files?	
In relation to the use of laptops, under what circumstances would personal data be held on them?	
Are laptops (and other portable devices storing personal data) password protected and appropriately encrypted?	

***Remote Access**:*

Do staff have remote access to IT systems containing personal data?	
Is the school/centre authority confident that such access is secure and governed by documented procedures?	
Does the school/centre system have a log/audit trail monitoring remote access?	

Network Security:

What type of back-up system operates?	
Is there a set daily/weekly procedure?	
Where are back-ups kept? Is this a secure location?	
Are all entry routes to server rooms / computer centre subject to security checks?	
Do existing measures relating to computerised data ensure that data may only be accessed by persons whose remit it is to access such data?	
Is there a log created of access to data? Are audit trails kept to ensure that only those who need to have access to the data are accessing the data?	
Are patterns of abnormal usage identifiable?	
Where patterns of abnormal usage are identified, are staff aware of how to handle this and are they aware of their obligations under the school's/centres Personal Data Security Breach Code of Practice?	
What security measures are in place relating to facsimile transmissions?	

15. Awareness and Responsibility

Refer to link: Auditing through a Compliance Checklist

How do you create awareness and responsibility amongst your personnel regarding the Data Protection Principles and the school's/centres Data Protection Policy?	

16. Governance:

Refer to links: What is Data Protection and why is it important for schools and select Responsibilities on schools/ETBs as data controllers

How is data protection compliance monitored throughout the school/centre?	
Are internal audits of data protection compliance conducted regularly?	
Who is responsible for implementing the Data Protection Policy?	

17. Data Security Breaches:

Refer to link: Storage & Security of Personal Data and also Personal Data Security Breach Code of Practice Form and Third party service agreements

Is school/centre management aware of its reporting obligations under the Data Protection Commissioner's Code of Practice in relation to data breaches?	
Would your school/centre be in a position to respond rapidly and appropriately to such a breach?	