Irish Youth Justice Service

Seirbhís na hÉireann um Cheartas i leith an Aosa Óig

Data Protection (Personal Data)

Guide for the Youth Justice Sector[1]

January 2011

[1]This document is intended for guidance only and does not purport to be a legal interpretation of the Data Protection Acts

Table of Contents

PART 1 Introduction to the Data Sharing Project

PART 2 The Guide

PART 1 - Introduction to the data sharing project

1. Establishment of the Irish Youth Justice Service

Following a review of the youth justice sector, the Government agreed a programme to implement youth justice reforms. The programme included the establishment of the Irish Youth Justice Service (IYJS) in 2007.

The Irish Youth Justice Service (IYJS) is an executive office of the Department of Justice and Law Reform with responsibility for leading and driving reform in the area of youth justice.

Working with the Office of the Minister for Children and Youth Affairs (OMCYA), the IYJS is guided by the principles of the Children Act 2001. The IYJS funds organisations and projects providing services, including Garda and Probation Projects, to young people aged under 18 years who find themselves in conflict with the law. These children may be involved with An Garda Síochána, the Probation Service and the Courts Service. The IYJS is also responsible for the management and development of children detention facilities.

The remit of IYJS includes improving the delivery of youth justice services and reducing youth offending. This challenge is met by focusing on diversion and rehabilitation involving greater use of community based interventions and the promotion of initiatives to deal with young people who offend. Providing a safe and secure environment for detained children and supporting their early re-integration back into the community is also a key function.

Following its establishment, the IYJS was tasked with developing the National Youth Justice Strategy.

2. The National Youth Justice Strategy

The National Youth Justice Strategy 2008-2010 was developed in consultation with key stakeholders.

The Strategy reflects the remit of IYJS - to provide a coordinated, strategic approach to service delivery for young people in trouble with the law. Putting services in place for this group of young people is the priority of the Irish Youth Justice Service.

The emphasis of the Strategy is on providing relevant services that meet needs and on delivering those services to high standards, while also having a positive impact on the community by reducing offending behaviour.

The Strategy is mindful of a child-centred approach to service delivery and outcomes, with the best interests of the child being paramount.

3. The Goals

The aim of the Strategy is to provide a co-ordinated approach amongst agencies working in the youth justice sector. Through a set of five high level goals, the National Youth Justice Strategy sets out the focus for agencies working in the youth justice sector. The priority for the Strategy is young people who have already been in trouble with the law and delivering the best outcomes for them and the community.

More specifically, the aim of High Level Goal 5 is:

- *To strengthen and develop information and data sources in the youth justice system to support more effective policies and services.*

One of the objectives (5.2) for the goal is:

- *Together with relevant statutory agencies, establish what information may be shared and the mechanisms for sharing it, where appropriate.*

The actions to achieve that objective include to:

- *Facilitate in so far as it can, the sharing and exchange of information in the best interests of the children in the youth justice system.*

The outcome of this action will be the:

- *Enhanced protection of the interests of children coming into contact with the youth justice system through the appropriate sharing of information.*

4. The Data Sharing Project

In order to provide a co-ordinated approach to service delivery, agencies need to share relevant personal data in relation to children.

This project to enable the sharing of personal information relating to children in the youth justice sector is based on High Level Goal 5 and objective 5.2 in the Strategy. The essence of the Goal is premised on a child-centred approach to service delivery and outcomes, with the best interests of the child being paramount.

The Strategy also provides that relevant legislation will be adhered to in the implementation of the Strategy. The attainment of the goal necessitates adherence to relevant legislation, in this case, data protection legislation.

To this end, the IYJS liaised and engaged with the Office of the Data Protection Commissioner throughout the project.

The Guide will apply to personal data held by the Irish Youth Justice Service and children detention schools. It is hoped that other organisations operating in the youth justice sector may find the principles as set out in the Guide useful in terms of providing practical direction and meeting their obligations under the legislation.

5. The Youth Justice Guide for organisations in the youth justice sector

In order to achieve the goal as set out in the National Youth Justice Strategy and to comply with data protection legislation, a general Guide has been developed for the youth justice sector. This sets out the general principles of data protection legislation.

Fairly obtaining personal information and fairly processing are fundamental principles of data protection.

Fairly obtaining includes letting the individual from whom personal information is being obtained know the use to which it will be put and to whom it will be disclosed - see section 8.1 of Part 2.

Fair processing (e.g. the use) of personal information will always take place with the consent of the young person (data subject) or by one of the permitted legal bases set out in the Acts - see section 8.1 of Part 2.

The sharing of personal information between organisations in the youth justice sector will occur in the main with the consent of the young person and/or of a person acting on his behalf.

However, in certain situations, notwithstanding that the young person has not consented to the sharing, the Acts permit limited sharing with a third party in particular situations. These issues are dealt with in more detail in Part 2 of the Guide - see section 8.3.

It is anticipated that this Guide incorporating the general principles of the legislation will remove any doubt about how and when the sharing of personal information is permitted and enable the sharing of personal information to take place to provide the best service possible to the child in a manner which is compliant with data protection law.

Appendix 1 attached to this Guide defines some of the technical terms used in data protection.

Data protection checklists to assist with basic compliance in relation to (i) obtaining, using and sharing information and (ii) organisational responsibilities are attached at Appendices 2 and 3 respectively.

A form which may be adapted for use by the various organisations working in the youth justice sector when sharing information with other organisations is attached at Appendix 4.

An explanatory leaflet for children and parents/guardians dealing with consent and a consent form which may be adapted for use are attached at Appendix 4.

A leaflet summarising the main points in relation to obtaining, using and sharing information which includes a chart outlining an organisation's main responsibilities is also available and can be downloaded from www.iyjs.ie

PART 2 - The Guide

6. Data Protection

A. Introduction to data protection:

Data protection is the means by which the privacy rights of individuals are protected in relation to the processing of their personal data. Personal data includes sensitive personal data.

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 both in electronic and manual form.

The general principle upheld by data protection legislation is that the individual (and/or her/his parents or guardians in the case of a child) is entitled to determine what personal information s/he gives to others and how this information is to be used. This right is subject to various qualifications to take account of the interests of others and of society as a whole.

The Data Protection Acts 1988 and 2003 have a significant role to play in the operational workings of organisations in the youth justice sector given the amount of personal and sensitive information held by them. The aim of this document is to ensure that each person employed in the various organisations that make up the youth justice sector has an understanding of the concepts of Data Protection and is aware of their own responsibilities. This, in turn, will assist both the Irish Youth Justice Service and the various organisations in protecting the data of young people. It also aims to provide guidance on the sharing of personal information in the youth justice sector in line with data protection legislation.

B. Office of the Data Protection Commissioner:

The Office of the Data Protection Commissioner was established under the 1988 Data Protection Act. The Data Protection Commissioner is responsible for upholding the rights of individuals as set out in the Acts, and enforcing the obligations upon organisations. The Commissioner is appointed by Government and is independent in the exercise of his or her functions. Individuals who feel their rights are being infringed can complain to the Commissioner, who will investigate the matter, and take whatever steps may be necessary to resolve it.

This Guide has been developed in consultation with the Office of the Data Protection Commissioner.

7. Definitions

This Guide describes how the Acts protect the rights of individuals in relation to their personal data (data subjects) mainly by placing duties on those who collect such data and decide how it is used (data controllers).

The term "organisation" rather than "data controller" and "individual" or "young person" instead of "data subject" are used where possible.

Whilst we have tried as far as possible to avoid using technical terms, in some instances, it will be necessary to consider the meaning of a relevant defined term to judge whether and how the Data Protection Acts apply.

This is particularly the case when dealing with the exemptions in relation to sharing personal information with third parties.

Accordingly, a 'definitions' section is contained at Appendix 1 of the Guide.

8. Data Protection Rules

There are eight rules which are central to protecting personal data.

The rules serve to protect the interests of individuals whose personal data is being obtained and used and also serve to protect the interests of the organisation collecting the data. They apply to everything that an organisation does with personal data.

These rules provide the key to complying with data protection law and if they are adhered to by an organisation, there is less scope for a claim to the Office of the Data Protection Commissioner that an organisation is in breach of the Data Protection Acts.

These rules are:

1. Obtain and process information fairly

2. Keep data only for one or more specified, explicit and lawful purpose(s)

3. Use and disclose data only in ways compatible with these purposes

4. Keep data safe and secure

5. Keep data accurate, complete and up-to-date

6. Ensure that data is adequate, relevant and not excessive

7. Retain data for no longer than is necessary for the purpose or purposes for which it was collected

8. Give a copy of his/her personal data to the relevant individual, on request

8.1. Obtain and process data fairly and lawfully (Rule 1)

This rule deals with *obtaining* and *processing* personal data. The definition of 'processing' (see Appendix 1) is very broad and most likely all actions taken by an organisation in relation to personal data will amount to processing.

For ease of use in this document, when 'processing' is referred to, it will broadly mean 'using'.

This rule is to a large extent about fairness which will usually be met by organisations being transparent - open and honest about their collection and use of personal data.

There will be circumstances when the purpose of information or data to be used is obvious, for example, details gathered from the child/parent on the child's admission to a children detention school. On other occasions it may be necessary to provide an explanation to the individual.

In certain situations, an individual has little option other than to supply information to the Probation Service or a detention school. In such circumstances it would be necessary for the employee of the organisation concerned to notify the individual of the purposes for collecting their data including any non obvious use of that information and take into account the individual's wishes regarding any additional use of the data. Individuals should be given the option of saying whether or not they wish their information to be used in these other ways.

Organisations in the youth justice sector will need to share relevant information with other organisations in the same sector for the purposes of providing a service to the young person in terms of their management, care and custody. The young person should be told that their information will be shared with the particular organisations concerned. If an organisation intends to make a significant change to what was originally consented to by the young person, then it would be prudent to obtain consent to the proposed new use.

This means that children should be made aware that their data will be shared with IYJS, the Probation Service, the Courts, other schools, the Irish Prison

Service and HSE as appropriate in the context of their management and their care and custody.

A. Obtaining data fairly

(a) In all circumstances, to fairly obtain data, the young person must, at the time the personal data is being collected, be made aware of:

(i) the name of the organisation,

(ii) the purpose(s) in collecting the data,

(iii) the persons or categories of persons to whom the data may be disclosed,

(iv) whether replies to questions asked are obligatory and the consequences of not providing replies to those questions and

(v) any other information which is necessary so that the collection of data may be fair.

B. Processing (i.e. Using) personal data

To fairly use personal data it must have been fairly obtained in line with (i) to (v) of A above and:

- the young person must have given consent to the use **or**
- the use must be necessary for one or more of a number of reasons as provided for in Section 2A of the Data Protection Acts and listed below.

It should be noted that these enabling conditions, other than consent, would not be general enablers covering all types of use of data within the Youth Justice sector.

Certain conditions as outlined below may be relied upon to enable specific and limited types of use in particular instances only.

Whilst consent will be the main enabler for the use of information by organisations in the youth justice sector, other enablers as listed hereunder could be used in particular circumstances, if appropriate.

Those most relevant which could apply to the youth justice sector include where the use of personal data is necessary:

(i) for compliance with a legal obligation, other than that imposed by contract;

(ii) to prevent injury or other damage to the health of a young person,

(iii) to prevent serious loss or damage to property of the young person,

(iv) to protect the vital interests of the young person where the seeking of the consent of the young person is likely to result in those interests being damaged,

(v) for the administration of justice,

(vi) for the performance of a function conferred on a person by or under an enactment,

(vii) for the performance of a function of the Government or a Minister of the Government,

(viii) for the performance of any other function of a public nature performed in the public interest by a person,

(ix) for the purpose of legitimate interests pursued by an organisation except where the use is unwarranted in a particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the young person.

It must be borne in mind that there is a distinction between the 'vital interests' of a young person and their 'best interests'. Whilst using data without the consent of the young person is permissible to protect their 'vital interests', using data in someone's 'best interests' where their consent has not been obtained would need a specific legal basis which does not currently exist in the Acts.

C. Processing (Using) sensitive personal data

The Data Protection Acts require additional conditions to be met for the use of sensitive personal data to be legitimate. Usually, this will be the *explicit consent* of the person to whom the data relates.

The use of sensitive personal data (and data will be sensitive data for the most part in the youth justice sector as it includes criminal convictions or the alleged commission of an offence), the data must have been fairly obtained in line with section A above and one of the conditions at B above must be met as well as additional requirements.

Accordingly, in order to use ‘sensitive personal data’ that has been fairly obtained (i.e. the data must have been fairly obtained in line with (i) to (v) of A above),

(i) the requirement for processing 'personal information' must be met;

and one of the following must be met:

(ii) the person has given explicit consent

or

the processing is necessary for one of the following reasons[2]:

(i) for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the organisation in connection with employment,
(ii) to prevent injury or other damage to the health of the young person or another person, or serious loss or damage to property or otherwise to protect the vital interests of the young person or of another person where consent cannot be given or obtained,
(iii) to prevent injury to or damage to the health of another person or serious loss or damage to the property of another person in a case where consent has been unreasonably withheld,
(iv) the information being processed has been made public as a result of steps taken by the young person;
(v) the processing is necessary for the performance of a function conferred on a person by or under an enactment, or
(vi) the processing is necessary for the performance of a function of the Government or a Minister of the Government, or
(vii) the processing is necessary for the purpose of obtaining legal advice, or in connection with legal proceedings, or is necessary for the purposes of establishing, exercising or defending legal rights, or
(viii) for medical purposes (and is undertaken by a health professional or a person who in the circumstances owes a duty of confidentiality to the young person that is equivalent to that which would exist if the person were a health professional).

Again, it should be noted that these enabling conditions, other than consent, would not be general enablers covering all types of use of data within the youth justice sector.

Certain conditions may be relied upon to enable specific and limited types of use in particular instances only.

[2] There are other conditions which are however, less relevant in the context of sharing information in the youth justice sector.

Explicit consent broadly means that the young person's consent must be absolutely clear. The consent obtained should cover the type of information, the specific use and any specific disclosures that might be made.

For further information on the issue of consent, see section 9 of this Guide.

8.2 Keep data only for one or more specified, explicit and lawful purposes (Rule 2)

The organisations in the youth justice sector may only keep data for a purpose/s that are specific, lawful and clearly stated and the data should only be used in a manner compatible with the purpose as advised (see 8.1). An individual has a right to question the purpose for which an organisation holds his/her data and the organisation must be able to identify that purpose.

In general, the various organisations in the youth justice sector (e.g. the IYJS, Children Detention Schools and the Probation Service) hold information for the purposes of the management, care and custody of young people who are in trouble with the law.

At the outset, organisations should seek to ensure that they are clear about the purpose or purposes for which they hold personal data so that they can ensure that any processing of that data (including use and disclosure) is compatible with the original purpose or purposes as required by Rule 3 - see 8.3 below.

Specifying the purpose or purposes of obtaining particular data at the outset is likely to help an organisation to be in a position to justify its use and disclosure of the data.

8.3 Use and disclose data only in ways compatible with these purposes (Rule 3)

A. Disclosure in ways compatible with the purpose for which the data was obtained

The Data Protection Acts place a limitation on the disclosure of personal data and it must not be used or disclosed for any purpose that is incompatible with the original purpose or purposes.

This is one of the reasons that it is important to establish the purpose in collecting data at the outset.

Disclosure in the context of data protection is the provision of personal data to a third party.

A third party in relation to personal data means any person other than:

- the young person;
- the organisation;
- any data processor (see definition at Appendix 1) acting further to an appropriate contract on behalf of the organisation which obtained the data.

An employee of one of the organisations in the youth justice sector acting in the course of their employment will not be considered to be a third party. This is because the person will be acting on behalf of the organisation in their capacity as employee of that organisation.

The Act places serious responsibilities on every employee of the organisations in the youth justice sector not to disclose data in relation to any individual to any other individual where consent is not given and there is no basis in the Data Protection Acts to do so (see exceptions at B below).

Personal data is used daily within the organisations in the normal course of operational functions. Any use or disclosure must be compatible with the purpose/s for which the data is collected and kept (except where a specific basis for its release applies).

An employee of any of the organisations making a disclosure should consider whether the young person would be surprised to learn that a particular disclosure is taking place. If the potential answer to this question is 'yes', then there is a need to question the basis for the disclosure prior to making it. This means that an organisation must seek to obtain the consent of the young person to the disclosure or establish if one of the exceptions permitted by the Data Protection Acts apply.

The provisions of the Data Protection Acts apply to the disclosure of personal data in any medium by a legal entity, i.e. paper, computer, network, web and phone.

The Data Protection Acts do not apply to the disclosure of data which is not personal data, i.e. aggregated or anonymised data or business information. Consideration should always be given to whether the request to obtain personal data can be met by the use of non-personal data such as a case conference to discuss the case without using the actual name of the individual.

B. Disclosures to a third party without the consent of the young person

An organisation shall not use or disclose personal data other than in ways that are compatible with the purpose for which the data was obtained.

A disclosure may be made to a third party where the disclosure is made at the request of, or with the consent of the young person or to a person acting on his behalf.

However, in certain situations, notwithstanding that the young person has not consented to the disclosure, the Acts permit limited disclosures to a third party to take account of where the individual's right to privacy must be balanced with other needs of civil society or where the disclosure is in the interests of the individual.

These exceptions are where the disclosure is required:

- for the purpose of safeguarding the security of the State;
- for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board;
- in the interests of protecting the international relations of the State;
- urgently to prevent injury or other damage to the health of a person or serious loss or damage to property;
- by or under any enactment or by a rule of law or order of a court;
- for the purposes of obtaining legal advice or for the purposes of, or in the course of, legal proceedings in which the person making the disclosure is a party or a witness;

You must consider each exception on a case by case basis because the exceptions only permit a departure from the requirements of the legislation to the minimum extent necessary in a particular instance.

As a disclosure may subsequently be challenged by a young person, an organisation should ensure that it will be in a position to defend its decision to apply an exception. It will therefore be prudent for organisations to ensure that

decisions about exceptions are taken at an appropriate level in the organisation.

These exceptions do not impose an obligation on a data controller to comply with a request for disclosure from a third party. Organisations are therefore, under no obligation to respond positively to the request for information.

In all cases where a disclosure of personal data is being made:

- the identity of the recipient of the disclosure should be established,

- the specific purpose of the disclosure should be established

and

- the legal basis/power to disclose the relevant data should be determined (This will be the consent of the individual or one of the exceptions permitted by the Acts as set out above).

A generic form which will seek to enable the sharing of data in compliance with the requirements of the legislation is available and may be adapted for specific use by the various organisations in the youth justice sector - see Appendix 5.

A record of all disclosures should be maintained.

In cases where there is any doubt as to disclosure, or the status of the data concerned, a file should be submitted to the Data Protection Co-Ordinator, IYJS. As appropriate, that person will then liaise with the Office of the Data Protection Commissioner.

Examples of legitimate disclosures are:

- from the Probation Service to IYJS and Children Detention Schools;
- from Children Detention Schools to the Probation Service and IYJS;
- from one Children Detention School to another Children Detention School where a child is being transferred or to the Irish Prison Service;
- to the Health Service Executive in respect of Child Welfare issues, etc.;
- to the Courts Service and other agencies with a statutory role in the youth justice sector;

- ❖ from Children Detention Schools or the Probation Service to their counterparts in another EU jurisdiction where a child is being transferred to that jurisdiction.

Accessing or disclosing personal data for any purpose other than that for which it was obtained is prohibited. Examples of this would be an employee of any organisation in the youth justice sector:

- accessing and/or disclosing details of any child, the knowledge of which the employee had obtained as a consequence of their work, to another person outside the organisation without the consent of the young person/parent or guardian and where there is no legal basis for the disclosure.

C. Disclosure through transferring personal data abroad

There are special conditions that have to be met before transferring personal data outside the European Union, where the receiving country does not have an EU approved level of data protection law. At least one of the following conditions must be met in that the transfer is:

- ❖ consented to by the young person,
- ❖ required or authorised under an enactment, convention or other instrument imposing an international obligation on this State,
- ❖ necessary for the purpose of obtaining legal advice,
- ❖ necessary to urgently prevent injury or damage to the health of a young person,
- ❖ part of the personal data held on a public register,
- ❖ authorised by the Data Protection Commissioner, which is normally the approval of a contract which is based on a EU model,
- ❖ the transfer is necessary for reasons of substantial Public Interest.

It is suggested that the advice of the IYJS Data Protection Co-Ordinator (see section 14) may need to be sought to ensure that these narrow conditions are correctly interpreted.

8.4 Keep data safe and secure (Rule 4)

Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction.

The security of personal information is all-important, but the key word here is appropriate, in that it is more significant in some situations than in others, depending on such matters as confidentiality and sensitivity and the harm that might result from an unauthorised disclosure. High standards of security are, nevertheless, essential for all personal information.

The nature of security used may take into account what is available, the cost of implementation and the sensitivity of the data in question.

The standard of security expected of all employees of organisations in the youth justice sector includes the following:

- access to the information restricted to authorised staff on a "need-to-know" basis in accordance with a defined policy,
- computer systems password protected,
- information on computer screens and manual files kept hidden from callers to offices,
- back-up procedures in operation for computer held data, including off-site back-up,
- all waste papers, printouts, etc. disposed of carefully by shredding,
- personal security passwords must not be disclosed to any other employee,
- all premises to be secure when unoccupied.

A designated person will be responsible for all of the above within each organisation with periodic reviews of the measures and practices in place (see section 13).

These should not be regarded as the full extent of an organisation's obligations in respect of confidentiality, safety and security.

Please see CMOD document *'Protecting the confidentiality of Personal Data'* at http://www.dataprotection.ie/documents/guidance/GuidanceFinance for comprehensive details on actions that should be taken.

The various organisations will ensure that appropriate data protection and confidentiality contractual clauses are in place with any processors of personal information on its behalf.

Safe and secure transmission of data

The safe and secure transmission of data is vitally important for organisations in the youth justice sector.

Regard should be had to the following:

- Data transfers should, where possible, only take place via secure on-line channels where the data is encrypted;
- Manual data transfers using removable physical media e.g. memory sticks, CDs, tape etc. should not take place;
- Strong passwords must be used to protect any encrypted data;
- Standard e-mail should not be used to transmit any data of a personal or sensitive nature.

These should not be regarded as the full extent of an organisation's obligations in respect of confidentiality, safety and security.

Please see CMOD document *'Protecting the confidentiality of Personal Data'* at http://www.dataprotection.ie/documents/guidance/GuidanceFinance for comprehensive details on actions that should be taken to ensure safe and secure transmission of data.

8.5 Keep data accurate, complete and up-to-date (Rule 5)

Apart from ensuring compliance with the Acts, this requirement has an additional importance in that the State may be liable to an individual for damages if it fails to observe the duty of care provision in the Acts applying to the handling of personal data.

To comply with this rule, each organisation will ensure that:

- ❖ clerical and computer procedures are adequate to ensure high levels of data accuracy,
- ❖ the general requirement to keep personal data up-to-date has been fully implemented,
- ❖ appropriate procedures are in place, including periodic review and audit, to ensure that each data item is kept up-to-date.

The Acts give a person a right to seek to have personal data amended or erased where it can be shown that it is factually incorrect. Examples of this are the updating of court outcomes to show the exact situation at any given time and ensuring that all biographical data, especially name and date of birth of a young person is correct.

8.6 Ensure data is adequate, relevant and not excessive (Rule 6)

The organisations in the youth justice sector can fulfil this requirement by making sure they only seek and retain the minimum amount of personal data needed for the specified purpose.

To comply with this rule, each employee should ensure that the information held is:

- adequate in relation to the purpose/s for which it is kept,
- relevant in relation to the purpose/s for which it is kept,
- not excessive in relation to the purpose/s for which it is kept.

The personal data kept should be enough to enable the organisation to achieve the specified purpose and no more. Personal information should not be collected or kept "*just in case*" a use can be found for the data in the future. Intrusive or personal questions should not be asked if the information obtained in this way has no bearing on the specified purpose for which personal data is held.

When requesting information from young people, it should be possible to answer YES to the following questions:-

1. Is the personal information held about individuals really necessary for the organisation to provide services?

2. Are individuals asked to provide just the information needed and no more?

3. Is there a good reason for asking individuals sensitive or personal questions?

For example, sometimes on forms and documentation, the Personal Public Service Number (PPSN) is requested from individuals as a matter of course.

However, it is not appropriate to seek the number routinely. There is a strict legislative 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 Protection manages the issuance and use of PPS numbers. A register of organisations that use the PPSN has been 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 .

8.7 Retain data for no longer than is necessary for the purpose or purposes (Rule 7)

This requirement places a responsibility on each organisation to be clear about the length of time data will be kept and the reason why the information is being retained. To meet this requirement, organisations should ensure that personal data is not retained for any longer than necessary.

All electronic and manual data will be retained in line with the policy on records management in each organisation.

All employees will be informed of the policy in respect of data retention by way of relevant Directives from their Data Administrator (see section 13) and shall ensure that all data under their control is managed and retained in line with the policy as established therein.

8.8 Give a copy of his/her personal data to the individual, on request (Rule 8)

Entitlements under an access request

Under section 4 of the Data Protection Acts, on making a written request, an individual about whom personal information is kept on computer or in a relevant filing system is entitled to:

(a) a copy of the data,

(b) a description of the purposes for which it is held,

(c) a description of those to whom the data may be disclosed and

(d) the source of the data unless this would be contrary to the public interest.

Although it may not apply in the youth justice sector, it is necessary to explain to an individual the logic used in any automated decision making process where the decision significantly affects the individual and the decision is solely based on the automated process.

This "right of access" is subject to a limited number of exceptions, which are listed below.

Each organisation should have clear co-ordinated procedures in place to ensure that all relevant manual files and computers are checked for the data in respect of which the access request is being made.

To make an access request, the young person (or former young person) must:

- apply to the relevant organisation in writing for access to their personal data,
- give any details which might be needed to help identify him/her and locate all the information the organisation may keep about him/her e.g. previous addresses, court dates, dates of detention etc,
- pay the appropriate access fee. (Organisations do not need to charge a fee but if one is charged, it cannot exceed €6.35.)

In response to an access request, each organisation must:

- supply the information to the individual promptly and within 40 days of receiving the request,
- provide the information in a form which will be clear to the ordinary person, e.g. any codes must be explained in ordinary language.

Where an access request is being refused or where some of the information is being withheld, the reasons for the refusal or part-refusal of the request must be clearly indicated in writing to the young person.

Responding to requests once a valid request is received (as above),

The relevant organisation must reply within forty days, even if personal data is not held or an exemption is relied upon.

There is no obligation to refund any fee that was charged for dealing with the access request if no personal data is found.

However, the fee must be refunded if the organisation does not comply with the request or if it is necessary to rectify, erase or supplement the personal data concerned.

Every individual about whom an organisation keeps personal information has a number of other rights under the Acts, in addition to the right of access.

These include the right to have any inaccurate information rectified or erased and the right to complain to the Data Protection Commissioner.

Circumstances where Access to Personal Data may be denied

The restrictions upon the right of access fall into five groups:

(i) The Data Protection Acts provide that the right of access does not apply in a number of cases, in order to strike a balance between the rights of the individual, on the one hand, and some important needs of civil society, on the other hand, such as the need to investigate crime effectively, and the need to protect the international relations of the State.

(ii) The right of access to medical data and social workers' data is also restricted in some very limited circumstances to protect the individual from hearing anything about himself or herself which might cause serious harm to his or her physical or mental health or emotional well-being.

(iii) The right of access to examination results is modified slightly.

(iv) The right of access does not include a right to see personal data about another individual, without that other person's consent. This is necessary to protect the privacy rights of the other person. Where personal data consists of expressions of opinion about the young person by another person, the young person has a right to that expression of opinion except where that expression of opinion was only given in anticipation of confidence and the provision of the Opinion would reveal the identity of the person who gave it.

(v) The obligation to comply with an access request does not apply:

- where it is impossible for the organisation to provide the data

or

- where it involves a disproportionate effort in the supply of the information. This would be unlikely to apply in the youth justice sector as the information regarding an individual is usually readily to hand.

Requests Made by Parents/Guardians

Children Subject Access Requests can be accepted from a child if, in the opinion of the organisation, the child has sufficient intellectual ability to understand the nature of the request.

A parent or guardian can exercise the right, and receive the reply if, in the opinion of the organisation:

- ❖ the child does not have the intellectual ability to understand the nature of the request, and

- ❖ the parent is acting in the best interests of the child, where such release to the parent would be appropriate and there is no information to suggest that the parents of the child are in dispute.

An access request on behalf of a child will not be acceded to if it would likely be relevant to any ongoing abuse/welfare allegations that may involve the requester.

Agents

Organisations may receive subject access requests by agents such as solicitors acting on behalf of a young person or former young person. The organisation should satisfy itself as to the identity of the agent and seek sufficient information about the individual s/he is acting for, to assist in establishing identity and locating the data sought.

The organisation will seek written confirmation from the individual authorising the agent to make the request. All responses will normally be sent directly to the young person at their home address as provided. Where a request is made for the information to go to a place other than the individual's home address, the relationship between the individual and the agent, will be a factor in determining whether to comply with the request. e.g. Client/Solicitor.

Further information about the right of access is available on the website of the Office of the Data Protection Commissioner (www.dataprotection.ie)

9. Consent

One of the conditions for using data is that the young person has given consent to the organisation collecting their personal data and its use for a particular purpose or purposes.

Age of consent

The Acts do not specify an age of consent. The nature of the consent required may vary from case to case and between implied and explicit having regard to whether the data involved constitutes sensitive personal data or not and the type of processing which is envisaged. If relying upon consent for the processing of personal data, the key test will be to demonstrate that consent exists. However, it is important that the young person appreciates the nature and effect of such consent. Therefore, different ages might be set for different types of consent.

Age of consent for sensitive personal data

When processing sensitive personal data, the level of consent must be explicit. This means that a young person must be aware of and understand the purposes for which his/her data are being processed. Explicit consent need not require a young person to sign a form in all cases. Consent can be understood to be explicit where a person volunteers personal data after the purposes in processing the data have been clearly explained. However, obtaining consent in writing after the purposes of obtaining the personal data have been explained may make it easier to demonstrate explicit consent if required to do so.

Consent by young persons

Where a person is unlikely to be able to appreciate the nature or effect of consent, by reason of physical or mental incapacity or age, then a parent, grandparent, uncle, aunt, brother, sister or guardian may give consent on behalf of the young person. These are the only circumstances in which a third party may give consent on behalf of a young person.

It is preferable to attempt, where possible, to obtain consent from both the young person and their guardian.

Factors which organisations should have regard to include:

- Consent of both guardian and young person (dual consent) should be obtained wherever possible.
- When obtaining consent from a young person, ensuring that they fully understand what he or she has given consent to, and the effects the sharing of such information may have.
- Where a young person is unlikely to be able to appreciate the nature or effect of consent by reason of age, then a parent or guardian may give consent.

To aid in obtaining full consent, a short explanatory leaflet for parents/guardians and children and consent form is attached at Appendix 4. The form can be signed by the relevant person(s) to indicate their consent to the use of their data. Parents/guardians and children should be given time to read this document **before** giving consent.

10. Data Processors

A Data Processor is a person or organisation who processes personal information on behalf of an organisation, but does not include an employee of the organisation who processes such data in the course of his/her employment.

As a minimum, any processing by a Data Processor should take place subject to a contract between the organisation and the processor which specifies:

- the purpose for which the data is shared with the processor and the conditions under which the data may be processed,
- that the data shared is for that specified purpose and that purpose only and cannot be used subsequently without consultation and permission from the relevant organisation,
- the security conditions attaching to the processing of the data and
- that the data be deleted or returned upon completion of the project or termination of the contract.
- that the processor receiving the information may not share it with other organisations without consultation and permission from the organisation from which the data was originally obtained,

The organisation engaging with the data processor is also required to take reasonable steps to ensure compliance by the data processor with these requirements. This may be by way of an audit for instance.

In the event that a data processor shares or handles data inappropriately, liability will fall upon the organisation providing the data in the first place.

11. Case conferences in relation to children

Where a parent/guardian is attending a case conference in relation to a young person and the young person has been made aware

- of the case conference,
- who will be in attendance and
- that their details are being discussed with the relevant personnel working to meet their needs,

no issue arises from the sharing of the minutes of the meeting with those attending to foster an integrated approach to the case.

Where a case conference not involving the attendance of the family takes place and the individual is not aware of or has not consented to his details being discussed/shared with third parties, data protection issues can arise where personal data is found to have been discussed and recorded on a file without the consent of the individual. These difficulties would also extend to sharing that data with others as the data has not been obtained fairly in the first place.

Therefore, it is important that at the outset of involvement with a young person, s/he is informed of the persons or categories of persons to whom their personal information will be disclosed.

12. CCTV

General

Recognisable images captured by CCTV systems are "personal data". They are therefore subject to the provisions of the Data Protection Acts.

An organisation needs to be able to justify the obtaining and use of personal data by means of a CCTV system. As CCTV infringes the privacy of the persons captured in the images, there must be a genuine reason for installing such a system. A system used to control the perimeter of a building for security purposes will usually be easy to justify. The use of CCTV systems in other circumstances – for example, to constantly monitor employees, customers or students – can be more difficult to justify and could involve a breach of the Data Protection Acts. An organisation also needs to be sure that it can meet its obligations to provide individuals with copies of images captured by the system.

Proportionality

All uses of CCTV must be proportionate and for a specific purpose. There will usually be no difficulty with the use of CCTV in schools for security purposes. However, its use must still be in compliance with the Data Protection Acts. Cameras placed so as to record external areas should be positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

The location of cameras is a key consideration when determining proportionality. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. Bedrooms, toilets and rest rooms are an obvious example. To justify use in such an area, an organisation would have to demonstrate that a pattern of security breaches had occurred in the area prior to the installation of the system such as would warrant constant electronic surveillance. Where such use can be justified, the CCTV cameras should never be capable of capturing images from cubicles or urinal areas.

Where organisations have any concerns about the positioning of CCTV cameras, they should liaise with the Data Protection Co-Ordinator in IYJS who will engage with the Data Protection Commissioner's Office in the matter, as appropriate.

Transparency

The relevant legislation requires that where CCTV is in operation, signage indicating its presence **must** be posted in the vicinity. The signage must be easily-read and well-lit and placed in prominent positions.

If the identity of the organisation and the usual purpose for processing – security - is obvious, all that needs to be placed on the sign is a statement that CCTV is in operation as well as a contact (such as a phone number) for persons wishing to discuss the processing. This contact can be for either the security company operating the cameras or the organisation. If the CCTV is for any other purpose in addition to security then this must be indicated on the signage.

Storage

When storing CCTV footage, organisations should note:

- The images captured should be retained for a maximum of one month, except where the image identifies an issue and is retained specifically in the context of that issue;
- Tapes should be stored in a secure environment with a log of access to tapes;
- Access should be restricted to authorised personnel. Similar measures should be employed when using disk storage, with automatic logs of access to the images created.

It is important to note that CCTV footage can be released as part of an access request, where it is relevant to the purpose for which data is being shared or to an individual making an access request.

13. Responsibility of Organisations

Senior Management

Senior Management in each organisation will ultimately have responsibility for the compliance of each employee with the Data Protection Acts.

These responsibilities include:

- ❖ overseeing the management of data protection matters within each organisation including if appropriate the appointment of a particular person to have overall responsibility, i.e. a Data Protection Administrator,
- ❖ ensuring that reporting lines exist to allow employees to raise matters relating to data protection at a senior level,
- ❖ managing the organisation's statutory obligations in respect of the Data Protection Acts including compliance with the Data Protection principles as set out in this Guide, registration with the Data Protection Commissioner and securing the rights of individuals under the Acts,
- ❖ maintaining an up-to-date knowledge of Data Protection legislation and general developments in other relevant areas (e.g. Freedom of Information Act) and to ensure that this Guide is disseminated and adhered to throughout the organisation,

- promoting data protection awareness through training, policy development, advice and guidance, ensuring that operating rules and general policy guidance in support of this Guide and all matters relating to the Acts are available to all staff,
- ensuring information and systems comply with the Data Protection principles and that appropriate security arrangements exist to protect data, including where necessary, that suitable contracts are drawn up relating to the processing of data by data processors,
- the investigation and resolution of complaints made in relation to personal data,
- providing for liaison on all data protection matters between the organisation and IYJS which will then liaise with the Data Protection Commissioner as appropriate.
- arrange for regular audits of compliance with all of the requirements outlined in this document.

<u>All employees of organisations working in the youth justice sector</u>

All employees have a duty to ensure compliance with the principles of Data Protection as set out and will undertake to follow the provisions of this Guide in accordance with policy and procedures.

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 done in accordance with the Data Protection Acts and this Guide.

Employees found in breach of the Data Protection Rules may be found to be committing an offence under the Data Protection Acts 1988 and 2003. S/he may also find themselves subject to the organisation's disciplinary policy. Furthermore, such members may be exposing themselves and the organisation to litigation from an injured party.

All current and former employees will be held accountable in relation to all data processed, managed and controlled by them during the performance of their duties.

14. Advice/Assistance

All files requesting advice and assistance on data protection issues within the youth justice sector should be directed to the Data Protection Co-Ordinator, IYJS, Montague Court, Dublin 2.

APPENDIX 1

Definitions

- '*personal data*' means data relating to a living individual who is or can be identified 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 person who controls the data (Data Controller).

  Examples of this are any report, statement, file or electronically recorded entry from which a living individual can be identified. An individual may also be identified by a unique pseudonym, a nickname, or some other characteristic or feature unique to them.

- *'Sensitive personal data*' relates to specific categories of data which are defined as data relating to a person's racial origin, political opinion or religious or other beliefs, physical or mental health, sexual life, criminal convictions or the alleged commission of an offence and trade union membership.

  Examples of this are files or entries containing details of charges, prosecutions or convictions relating to an individual.

- A '*data controller*' is the individual or the legal person (organisation) who controls and is responsible for the keeping and use of personal information on computer or in manual files.

  A data controller can be an individual, a legal entity such as a company, Government Departments or a voluntary organisation. Examples of cases where the data controller is an individual includes general practitioners, pharmacists, politicians and sole traders, where these individuals keep information about their patients, clients and constituents.

  All data controllers must comply with certain rules about how they collect and use personal information.

- A *data processor* means a person who processes information on behalf of a data controller but it does not include an employee of a data controller who processes such data in the course of his/her employment. For example, if IYJS outsourced particular work, the Acts would place certain responsibilities via a written contract on such entities in relation to their processing of personal data.

- *Manual data* means information which is kept as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

Examples of this are all traditional paper files such as individual case files relating to children and notes made at case conferences relating to children.

- *Automated data* means broadly speaking, any information on computer, or information recorded with the intention of putting it on computer.

  Examples of this are entries made on the computer system on the remand or committal of children to children detention schools.

- *Relevant Filing System* means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily accessible.

  Examples of this in Children Detention Schools are Filing Systems in respect of individual children

- *Access Request* is where a person makes a written request to a data controller for the provision to them of a copy of their personal data under section 4 of the Acts.

- *Processing* means 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.

  This, in effect, means that every time an employee records an entry in their personal notes such as their notebook, on an official record, on a manual file such as a young person's file or on a computerised database regarding a living individual or individuals who can be identified from the data, the employee is deemed to be processing the data.

- *Data Subject* is an individual who is the subject of personal data, e.g. the young person.

- *Employee* means an official of the Irish Youth Justice Service or an official of a Children Detention School.

APPENDIX 2

Basic Data Protection Checklist [3]

Obtaining, Using and Sharing Personal Information[4]

This short checklist will help you comply with Data Protection requirements. While being able to answer 'yes' to every question does not necessarily guarantee compliance, it does mean that you are heading in the right direction.

Obtaining the Information Fairly

Have you:

- identified yourself?
- told the individual the reason why you want their information?
- told the individual the organisations to which you will disclose their information?
- given any other information necessary to be fair to the individual.

Adequate, relevant and not excessive

- Have you identified the reason why you are asking for sensitive or personal data?
- Are you seeking only the minimum amount necessary?

Using the Information

Have you:

- obtained the consent of the individual to the use?

or:

- established if one of the enabling conditions apply? (Refer to the Data Protection Guide for the Youth Justice Sector - section 8.1.)

Sharing/Disclosing the Information with Other Organisations

- Has the individual been informed of the disclosure and consented?

or:

- Does one of the permitted exceptions contained in section 8 of the Acts apply? (see section 8.3 of the Guide)

If you cannot answer yes to either of the above, then you must go back to the individual and obtain their consent before you can share the information.

[3] For further information, please refer to the Data Protection Guide for the Youth Justice Sector

[4] See also the Organisational Checklist

APPENDIX 3

Basic Data Protection Checklist: Organisational Concerns[5]

This short checklist will help an organisation to comply with Data Protection requirements. While being able to answer 'yes' to every question does not necessarily guarantee compliance, it does mean that the organisation is heading in the right direction.

Keeping data for a specified, explicit and lawful purpose

- Are you keeping the data in line with the purpose you identified at the outset?

Safety and Security

- Are you satisfied that the personal information is being held securely?
- Are the appropriate security measures in place both internally and externally (if transmission is taking place)?
- Is access to personal information limited to persons on a strict need to know basis?

Accurate, complete and up-to-date

- Is the personal information accurate and up-to-date?
- Do you know how much information is time-sensitive?

Retention

- Is a defined policy on retention periods for all items of personal information in place?
- Do you delete/destroy personal information as soon as you no longer have a need/use for it?

Right of Access

- Would you know what to do if a young person asked for a copy of the information that you hold about them?
- Are you in a position to respond within 40 days?
- Are you in a position to provide a copy of all personal data held including copies of CCTV images?

For further help or information please refer to the Data Protection Guide for the Youth Justice Sector.

[5] See also the Checklist for obtaining, using and sharing personal information

APPENDIX 4
An Explanatory Guide for Parents and Children in relation to Consent

1. Introduction

In order to achieve the best outcomes for children in the youth justice sector, personal information is required. This aids staff in providing a service appropriate to the individual child. We obtain your personal information from you with your agreement and will only give that information to other organisations with your agreement except where there is a clear legal basis to provide data to another organisation. This leaflet seeks to inform you of the effect of giving your consent. Parents and children are advised to read this leaflet before giving consent. You may also wish to take the opportunity to raise any issues of concern to you.[6]

The details of what information is sought from you, what it will be used for, and who such data will be shared with are set out on the consent page attached to this document.

2. Sharing Your Data

[Name of organisation] liaises with other organisations in the youth justice sector on a frequent and recurring basis in order to provide the best service to children. In our day to day practice, it may be necessary to share personal data with such organisations.

Signing the attached form will indicate your consent to sharing relevant data with the organisations named on the form. In the event that we need to share data with any other organisations, we will explain the reasons why such data needs to be shared and provide a further consent form for you to sign.

Personal data will not be released to others without your consent.[7]

3. Who May Give Consent

The law does not specify an age of consent in relation to a child sharing their personal data. In the interests of best practice, we prefer to obtain the consent of the parent and the child. Places for both parents and children to sign have been set out on the attached form, with a third signature for a witness (who will be an employee of the organisation seeking your consent).

---

[6] For full details on your rights under Data Protection Law, you may wish to contact the Office of the Data Protection Commissioner.

[7] There are some limited exceptions which allow disclosure to a third party without obtaining the consent of the individual - See section 8.3 of the Youth Justice Guide. You may wish to discuss these with the person seeking your personal data or the person with responsibility in the organisation for data protection matters.

However, if a child is unlikely to be able to appreciate the nature or effect of consent, by reason of physical or mental incapacity or age, then a parent, grandparent, uncle, aunt, brother, sister or guardian may give consent on behalf of the child.

CONSENT FORM
[NAME OF BODY]

FULL NAME OF CHILD: _____

FULL NAME OF PARENT OR GUARDIAN: _____

INFORMATION SOUGHT: _____
(List) _____
_____
_____
_____
_____
_____
_____
_____
_____

PURPOSE: _____
_____
_____
_____
_____
_____
_____
_____

BODIES OR ORGANISATIONS WITH WHOM DATA WILL BE SHARED: _____
_____
_____
_____
_____
_____

I have read the above guide and understand that giving consent will mean that my personal data will be used for the purpose(s) stated and shared with the relevant listed organisations.

Signed: _____ **Date:** _____
Child

_____ **Date:** _____
Parent or Guardian

_____ **Date:**_____
Witness & Position in Organisation

APPENDIX 5
{INSERT NAME OF ORGANISATION}
DATA PROTECTION FORM

FOR SHARING DATA WITH OTHER ORGANISATIONS

Please note data is only provided on the basis detailed below:

NAME OF INDIVIDUAL (DATA SUBJECT): _____

PERMANENT ADDRESS OF INDIVIDUAL: _____
_____
_____
_____

CONSENT OF THE INDIVIDUAL: _____ (Yes/No)
or
EXCEPTION applies (state relevant one)[8] _____
_____
_____

DATA PROVIDED: (List all) _____
_____
_____
_____
_____
_____
_____
_____
_____

FOR THE PURPOSE OF: (List all) _____
_____
_____
_____
_____
_____
_____

PROVIDED TO: _____
_____
_____

[8] See section 8.3 of the Youth Justice Guide for permitted exceptions allowing disclosure without consent.

_____

DATE PROVIDED: _____

METHOD OF PROVISION OF DATA: _____

Please note:

(i) The data provided is for the stated purpose only. Any other uses will be outside your remit and may result in a breach of Data Protection legislation and liability under the Acts.
(ii) The data provided cannot be shared with other external organisations without consultation and permission from our organisation.
(iii) The data shall be stored securely.
(iv) In discharging our obligations under data protection, we also expect that your organisation complies with data protection law in general.

Any violation of the above terms may result in the bringing of a complaint to the Data Protection Commissioner by an individual or other action.

If you have any queries, or suspect a breach of data protection law in relation to a child's personal data, please contact me at **{CONTACT DETAILS HERE}**:

Signed: _____Date: _____
{NAME HERE}, Data Protection Co-ordinator
(Name of organisation)

INDEX