

INFORMATION MANAGEMENT POLICY

Final Version, Ref, OCDC12

Document Title	Information Management Policy
Version	Final V 1.0
Owner	Director, Oberstown
Approved by	Board of Management
Date	19.07.2017 18.10.2018 (Approved Extension) 10.09.2019 (Approved Extension)
For Review	31.01.2020

1. Purpose of Policy

The purpose of this policy is to set out a framework for best practice in the area of information management and security in order that Oberstown, and the information held by Oberstown is protected. This policy sets out the rules for expected behaviour by staff at Oberstown in order that legislative requirements are upheld and that risk to the organisation is minimised.

2. Policy statement

Good information governance supports the delivery of person-centred¹, safe, high quality care and ensures that when sharing information across services, service providers protect and manage personal information in a sensitive and responsible manner.²

In Oberstown, information should be protected from unauthorized access, modification, disclosure, and destruction.³ In line with Oberstown's purpose and function, information must be created, collected and stored proportionate to the organisations needs and adhere to legislative and regulatory requirements.⁴

At Oberstown:

- information should be treated as an organisational asset and all staff members of Oberstown must maintain the confidentiality of information obtained both during and after employment.
- data about staff members, young people and their families, including personal health information should be collected, used and shared securely and in line with legal requirements and data protection requirements.
- Data should be retained for no longer than is necessary and should be held only for the purposes for which it was collected, i.e. the data should be relevant and not excessive.
- information should be maintained so that it is available, accessible and trustworthy accurate, valid, reliable, timely, relevant, legible and complete.
- All staff members must take personal responsibility for the information they create, capture or maintain.
- All staff members must ensure that they are always aware of and respect the confidentiality of information they produce, share or receive.
- Take appropriate measures to protect information, including personal information, which cannot be shared for reasons of security or privacy.⁵

¹ A person-centred approach to data collection focuses on the needs and privacy of the individuals about whom the data is recorded and ensures that the privacy, confidentiality and quality of personal health information is assured and that national health and social care data collections collect, use and store data and information in a safe and effective way.

² *Guidance on information governance for health and social care services in Ireland*, <https://www.hiqa.ie/sites/default/files/2017-01/Guidance-on-information-governance.pdf>

³ Peltier, Thomas, R. "Information Security Fundamentals."

⁴ Dept of Finance, Protecting the confidentiality of Personal Data Guidance Note, 2008. Available at: <https://www.dataprotection.ie/documents/guidance/GuidanceFinance.pdf>

⁵ Young people and their families will be informed of how their personal health information is used through a statement of information practices.

Confidential information regarding Oberstown's practices and procedures or personal information about young people, their families and employees must not be posted or discussed on the Internet, including inter alia, social networking sites, discussion forums, message boards or internet chat rooms.

Except where permission has been sought and received from the director of Oberstown, staff should not engage with media or other organisations who may be seeking information or official comment about Oberstown.

Staff should be aware that comments made while off-duty and online are also governed by privacy and data protection requirements and basic duty of care standards still apply.⁶

3. Scope of Policy

This policy covers all aspects of holding, obtaining, recording, using, sharing and disclosing of Data and information or records. Records can come in a variety of forms including: paper documents including both written and printed matter, electronic records (i.e. word processing files, data base, spreadsheet files, emails, electronic data on any media etc) photographs, or anything on which information is recorded or stored.

4. Legal framework

It is the principal aim of Oberstown Children Detention Campus under s 158 of the Children Act 2001 to provide appropriate educational and training programmes for children referred to the Campus by a court and to promote their reintegration into society as persons who are capable of making a positive and productive contribution to society. This must be secured by having regard to young people's health, safety, welfare, interests; providing them with proper care, guidance and supervision; preserving and developing young people's relationships with their families; exercising proper moral and disciplinary influences on young people and recognising their personal, cultural and linguistic identity.

According to s 180 of the Act, young people in Oberstown are in the lawful custody of the Director who is 'to do what is reasonable...in all the circumstances for the purpose of safeguarding or promoting the child's... health, development or welfare'.⁷

These obligations are fulfilled, among other means, through the implementation by staff of Oberstown's policies and procedures.

The maintenance of privacy and confidentiality of individuals is underpinned by a number of legislative provisions.

As per s. 252 of the *Children Act, 2001*, nothing shall be published or broadcast that leads to the identification of a young person.

Privacy and confidentiality is also protected under the requirements of the *Data Protection Acts 1988 and 2003*, and the *Freedom of Information Acts 1997 and 2003*. Oberstown must also adhere to the provisions of the National Vetting Bureau (Children and Vulnerable Persons) Act.

Furthermore, staff must safeguard information as per their obligations under the *Official Secrets Act*. However, the *Protection for Persons Reporting Child Abuse Act, 1998*⁸ ensures that there are no barriers for persons wishing to report a concern about child abuse or welfare to Tusla or An Garda Síochána. The *Protected Disclosures Act, 2014* also applies to all sectors, public and private, who make a 'protected disclosure' in respect of certain unlawful activities – 'relevant wrongdoings' – they believe are occurring.

⁶ For information on Internet usage generally while at work, staff should refer to section 47 of the Employee Handbook.

⁷Section 180(8)(b) Children Act 2001.

⁸ *Protection for Persons Reporting Child Abuse Act, 1998*.

Furthermore, the *Criminal Justice (Forensic Evidence and DNA Database Systems) Act 2014*, allows that DNA samples be taken from young people convicted of an offence and sentenced to Oberstown. The legislation sets out what the DNA will be used for, and for how long it will be held.

Oberstown receives information from a variety of sources. The retention of data is allowed for in certain cases as set out in Part 2 of the *Data Protection Acts 1988 and 2003*. The practical expression of the law in this respect regarding young people in detention is set out in Schedule 1 & 2 of the IYJS Record Management Policy.⁹

4.1 Human rights standards

The United Nations Convention on the Rights of the Child (UNCRC), to which Ireland is a party, sets out the rights to which all children, including children in detention, are entitled.¹⁰ The Convention requires that all children are entitled to enjoy their rights without discrimination, they must have their best interests taken into account in all matters concerning children and have their views taken into account in all matters affecting them in line with their age and maturity. Under Article 40 of the Convention, every young person in conflict with the law has the right to be treated in a manner consistent with the promotion of their sense of dignity and worth, which reinforces the respect for the human rights and fundamental freedoms of others and which takes into account the young person's age and the desirability of promoting reintegration and assuming a constructive role in society.

The Committee on the Rights of the Child has expressed concern about the lack of data relating to young people in conflict with the law.¹¹

As per the legal requirements set out above, data collection and research should be balanced with young people's privacy and confidentiality. These issues are also set out in the European Guidelines on Child-friendly Justice (2010).¹²

Ireland is also a party to the Convention for the Prevention of Torture and Inhuman and Degrading Treatment and Punishment (CPT) and to the European Convention on Human Rights (ECHR), both of which are relevant to children deprived of their liberty. Under the *ECHR Act 2003*, 'organs of the state' are required to act in a manner consistent with obligations under the ECHR. Article 8 of the ECHR guarantees the right to respect for private and family life, home and correspondence.¹³

5. Definitions

Data Protection is the safeguarding of the privacy rights of individuals in relation to the gathering and processing of personal data.

The definition of a **record** is documentary evidence, regardless of form or medium, created, received, maintained and used by the organisation in pursuance of its legal obligations or in the transaction of business. This definition draws a distinction between a record and a document – a record is a final version that may be retained, while a document can be changed and will not normally be retained, except for audit trail purposes where necessary.

⁹ IYJS, Record Management Policy, 2011. Available at:

<http://www.iyjs.ie/en/IYJS/Record%20Management%20Policy%20IYJS.pdf/Files/Record%20Management%20Policy%20IYJS.pdf>

¹⁰ Available at: <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx>

¹¹ UNCRC, General Comment No.10, Children's Rights in Juvenile Justice. Available at:

<https://www.un.org/ruleoflaw/blog/document/childrens-rights-in-juvenile-justice-committee-on-the-rights-of-the-child-general-comment-no-10/>

¹² Council of Europe. Guidelines of the Committee of Ministers of the Council of Europe on child-friendly justice. Available at <https://rm.coe.int/16804b2cf3>

¹³ ECHR, available at: http://www.echr.coe.int/Documents/Convention_ENG.pdf

Personal health information is data relating to an 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. The term personal health information is broad and includes such matters as personal information relating to the physical or mental health of the individual, as well as any genetic data or human tissue data that could be predictive of the health of the individual or his or her relatives or descendants. In essence, it covers any information relating to an individual that is collected for or in connection with the provision of a health or social care service.¹⁴

Privacy can be defined as the right of individuals to keep information about them from being disclosed. Confidentiality refers to a duty that a person owes to safeguard information that has been entrusted to him or her by another.

6. Related Documentation

- Oberstown Staff handbook.
- Protected Disclosures policy and procedure.
- Guidance on information governance for health and social care services in Ireland.¹⁵
- IYJS, Data Protection Guide for the Youth Justice Sector.¹⁶

¹⁴ <https://www.hiqa.ie/sites/default/files/2017-01/Guidance-on-information-governance.pdf>

¹⁵ <https://www.hiqa.ie/sites/default/files/2017-01/Guidance-on-information-governance.pdf>

¹⁶ IYJS, Data Protection Guide for the Youth Justice Sector, Available at:
<http://www.iyjs.ie/en/IYJS/Data%20Protection%20YJ%20Guide%20-%20Jan%2011%20Final.pdf/Files/Data%20Protection%20YJ%20Guide%20-%20Jan%2011%20Final.pdf>