St. Michael's House

DATA PROTECTION POLICY incorporating :-

APPENDIX 1 POLICY FOR THE RETENTION OF RECORDS.
APPENDIX 11 SUBJECT ACCESS REQUESTS
APPENDIX 111 DATA BREACHES MANAGEMENT

Written By:	....	**DPO SMH and external DPO (Xpert DPO)**
Reviewed By:	....	**Tom Mitchell FOI and DPO Admin**
Approved By:	....	
		Signed: ***Liz Reynolds, C.E.O.***
Effective From:	....	**01 Jan 2024**
Reviewed:	....	**This Policy will be reviewed and updated on an ongoing basis**
		Signed:
Next Review Date:	....	**01 Jan 2027**
Distributed To:	....	**All Organisation**
Monitoring Mechanism:	....	**Data Protection Officer and DPO Admin Office**

Person Centred • Professional • Honest • Ethical • High Standards of Governance • Innovative
All Policies and Procedures are in line with *St. Michael's House* ***Values***

ST MICHAEL'S HOUSE DATA PROTECTION POLICY incorporating :-

APPENDIX 1 POLICY FOR THE RETENTION OF RECORDS

APPENDIX 11 SUBJECT ACCESS REQUESTS

APPENDIX 111 DATA BREECHES MANAGEMENT

1 INTRODUCTION TO DATA PROTECTION POLICY

Pursuant to the provisions of the GDPR (EU Regulation 2016/679) and the Data Protection Act 2018, the Board of Directors of St. Michael's House has approved the following Data Protection Policy

Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e., living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

Definitions used by St. Michael's House (drawn from the GDPR)

Article 2 from the General Data Protection Regulation

Material scope

–GDPR applies to the processing of personal data wholly or partly by automated means (i.e., by computer) and to the processing other than by automated means of personal data (i.e., paper records) that form part of a filing system or are intended to form part of a filing system.

Article 3 from the General Data Protection Regulation

Territorial scope – the GDPR will apply to all Data controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU, that process personal data, in order to offer goods and services or monitor the behaviour of data subjects who are resident in the EU.

Article 4 from the General Data Protection Regulation

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal Data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Special Categories of Personal Data (also known as Sensitive Personal Data) – Which are highly relevant as they require higher level of protection. This is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

Data Controller – the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data Processor – means a natural or legal person, public authority, agency, or other body that processes personal data on behalf of a data controller.

Data Subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not, by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. The relevant legal basis for processing of special category data in Irish law for Articles 9(2)(h) is Section 52 (as there is a lack of Ministerial regulation. Not all our workers are health practitioners as required by Section 52. The duty of confidentiality is enshrined in all contracts of employment of those processing data, for example care workers, care assistants, secretaries, receptionist, administrators, office managers, instructors etc.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal Data Breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data Subject Consent - means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Third Party – a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

2. Policy statement

The Board of Directors of St Michaels House, Ballymun Rd, Ballygall, Dublin 9 is committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information St. Michael's House collects and processes in accordance with the General Data Protection Regulation (GDPR).

The aim of this document is to provide a working understanding of the requirement on St Michael's House and its staff in ensuring compliance and adequate safeguards are put in place to protect the fundamental rights and freedom of service users and staff.

Compliance with the GDPR is described by this policy and other relevant policies such as the Information Security Policy along with connected processes and procedures. These policies can be viewed on our policy section on our website.

The GDPR and this policy apply to all of St. Michael's House's personal data processing functions, including those performed on employees' and suppliers' personal data, and any other personal data the company processes from any source.

The Data Protection Officer is responsible for reviewing the record of processing activities, in the light of any changes to St. Michael's House's activities (as determined by changes to the records of processing activities / data inventory) and to any additional requirements identified by legal requirements and by means of data protection impact assessments. This record needs to be available on the supervisory authority's request.

This policy applies to all Employees and Staff of St. Michael's House, including outsourced suppliers. Any breach of the GDPR will be dealt with by St. Michael's House's Director of Human Resources and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Contractors and any third parties working with or for St. Michael's House, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy.
No third party may access personal data held by St Michael's House **without having first entered into a Data Processing Agreement**, which imposes on the third-party obligations no less onerous than those to which St. Michael's House is committed, and which gives St. Michael's House the right to audit compliance with the agreement.

3 Personal Data

St Michael's House collects and processes 'personal data' and 'special category data', as defined under the General Data Protection Regulation, in order to, deliver its services. This information relates to past, current, and future services users, employees, volunteers, suppliers, and others with whom staff may communicate within the course of their work. All data collected may be used to procure services for service users, past and present, within St Michaels House and outside of St Michaels House. In addition,

staff maybe required to collect and use certain types of personal information and or special categories of personal data to comply with legal requirements. Such as the Child First Act 2015, ensuring child protection and welfare when reporting an incident to Tusla, HIQA requirements or notifications etc.

The Personal Data records held by St. Michael's House may include:

4. **Service Users Data**

Categories of service users Data :
Personal details about people who use St Michaels House's residential, respite, day, and clinic services **:-**
such as contact names, date of birth, address, next of kin, telephone numbers, email, country of birth, photographs, videos, attendance records, medical card number, social preferences, sleep and spiritual needs, clinical needs, daily records, and personal planning records. Relevant information from other health and social care professionals, including information on diagnosis and assessments, interventions, and other relevant information on diagnosis and assessments, interventions and supports and other relevant information relative to personal care needs. Other relevant information in relation to finances / bank statements accident / incident reports and correspondences between service professionals.

a) Purposes :

Processing Notice on Patient / Service Users Information Fair Processing

The three areas are:

- To manage and deliver care (Direct Care)
- To improve services and plan for the future (Indirect Care) e.g. clinical audit
- To understand and develop new treatments and techniques (Research).

As per Article 6 (1) (e) and Article 9 (2) (h) of the GDPR, once this notice is made available to patients and service users, further processing of this data in accordance with the Fair Processing Notice does not require consent of the patient or service user, except of course where consent is required for research.
It should of course also be noted that any such further processing of the data that is necessary in the fulfilment of the organisations' role in delivering and managing health and social care services should not adversely affect the freedoms and rights of the patient/service user (data subject).

Service users' Data records are kept for the purpose of :-

Data relating to service users:

The lawful basis for the transfer of service user files is underpinned by the Health Acts 1947-2020 & under GDPR 6.1(e) [public interest] & 9.2 (h) section 52 of the Data Protection Act 2018 where the processing "is undertaken by or under the responsibility of (a) a health practitioner (as defined in the Health Identifiers Act 2014) or (b) a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which would exist if that person were a health practitioner" [provision of care].

The information that we collect about you may include details such as:

- Name, address, telephone, email, date of birth and next of kin

- Any contact we have had with you through appointments and hospital attendances
- Details and records of treatment and care, notes and reports about your health, including any allergies or health conditions
- Results of diagnostic tests, e.g. x-rays, scans, blood tests
- Financial and health insurance information
- Other relevant information from people who care for you and know you well, e.g. health professionals, relatives and carers.
- We may also collect other information about you, such as your sexuality, race or ethnic origin, religious or other beliefs, and whether you have a disability or require any additional support with appointments (like an interpreter or advocate).
- CCTV and security information.

Why do St Michael House collect information about you ?
To make sure you get the best care, doctors, nurses and the team of healthcare staff caring for you, keep records about your health and any care or treatment you may receive from us. It is important for us to have a complete picture as this information enables us to provide the right care to meet your individual needs.

How we store your personal data
Your information is collected in a number of different ways. This might be from a referral made by your GP or another healthcare professional you have seen, or perhaps directly from you - in person, over the telephone or on a form you have completed. There may also be times when information is collected from your relatives or next of kin e.g. if you are taken to our emergency department (A&E) but you are very unwell and unable communicate. During your treatment health specific data will be collected by the doctors, nurses and healthcare staff taking care of you and will be held in your patient chart (This can be paper and/or electronic).

How we store your personal data ?
Under GDPR, strict principles govern our use of personal data and our duty to ensure it is kept safe and secure. Your data may be stored within electronic or paper records, or a combination of both. All our records have restricted access controls, so that only those individuals who have a need to know the information can get access. This might be through the use of computer passwords, audit trails and physical safeguards e.g. security controlled access.

How we use your information and why this is important ?
We use your information **to manage and deliver your care (Direct Care)** to ensure that:

- The right decisions are made about your care
- Your treatment is safe and effective; and
- We can coordinate with other organisations that may be involved in your care.

This is important because having accurate and up-to-date information will assist us in providing you with the best possible care.

In addition to using the data to provide for your care, this data is also routinely used **to improve services and plan for the future (Indirect Care)**, therefore, your data may be used in:

- Evaluating and improving patient safety

- Reviewing the care provided to ensure it is of the highest standard possible, improving individual diagnosis and care. This can be carried out by multiple quality improvement methods e.g. clinical audit.
- Training healthcare professionals
- Ensuring that our services can be planned to meet the future demand. E.g. analysing peak times, staffing levels and average length of stay, projected demand by disease/condition.
- Preparing statistics on hospital performance and monitoring how we spend public money
- Supporting the health of the general public e.g. Influenza, winter vomiting bug.

- **The activities listed above are part of normal delivery of care and under GDPR your consent is not required**. However, we recognise our duty to always keep your data secure and confidential and where appropriate we de-identify your data when using it for improvement. Using the data to understand and develop new treatments and techniques (Research). Research in healthcare is vital in helping develop understanding about health risks and causes to develop new treatments. It is usual for patient information to be used for research. **Your consent will be sought prior to being asked to participate in a research study** or to have your personal data used in a research study. In some circumstances, consent exemptions may be granted by the Health Research Board Consent Declaration Committee (HRBCDC). You will not be identified in any published results without your prior agreement.

Up to date and accurate information obtained is used to manage and deliver health and social care while enduring the right decision are made about service users care, ensuring their treatment is safe and effective, and to also guarantee proper coordination with other organisations that may be involved in their care.

Reviewing the care provided to ensure it is of the highest standard possible, improving individual diagnosis and care. To investigate complaints, legal claims, or adverse incidents To communicate with service users and their next of kin. To deliver information about St. Michael's House and its services where an individual has subscribed to receive same.

b) Lawful bases for processing
- Consent
- Necessary for the execution of contractual obligations
- Statutory Obligations (e.g., payment of payroll taxes etc.)
- Vital Interest
- Necessary for Legal Obligation
- Public Tasks
- Legitimate Interest

c) **Location and Security procedures of St Michael's House**

Manual records are kept locked and secured in all locations under the control of St Michael's House.

Digital Records are stored on servers which can only be accessed by password protected computers and laptops with adequate encryption and firewall software. Other electronic data is held on secure servers.

All mobile phones are password protected and encrypted.

d) **To prevent the loss of personal Data** while being transported to and from St Michael's House, employees working remotely may only have personal Data on laptops with adequate encryption and firewall software. Manual records brought home for work are the sole responsibility of the person bringing them home . They must be kept securely at all times If this data is lost or stolen it must be reported immediately.

5 Staff Records

Categories of Staff Data

As well as existing members of staff (and former members of staff), these records may also relate to applicants applying for positions within the company, trainee staff and staff under probation.

These staff records may include :

- Name, address and contact details, date of birth, PPS number.
- Name and contact details of next-of-kin in case of emergency.
- Banking details, pension records
- Data relative to recruitment processes : Application forms, CV's, References, Gardai vetting, declarations, professional qualifications, and registrations.
- Images and videos of staff that are used for promotional purposes.
- Details of approved absences (career breaks, parental leave, study leave, etc)
- Details of work record (qualifications, courses attended etc)
- Detail of any accidents / injuries sustained on company property or in connection with the staff member carrying out their duties.
- Occupational health data
- Driving licence and motor insurance details
- Next of Kin and in case of Emergency contact number

a) Purposes:

Staff Records are kept for the purposes of :

- The management and administration of St. Michael's House as an organisation (now and in the future)
- To facilitate the payment of staff, and calculate other benefits/entitlements (including reckonable service for the purpose of calculation of pension payments, entitlements and/or redundancy payments where relevant)
- Human resources management.
- Recording promotions made (documentation relating to promotions applied for) and changes in responsibilities, etc.
- To promote St Michael's House online and at industry events as a broadband provider.
- To enable St. Michael's House to comply with its obligations as an employer, including the preservation of a safe, efficient working and teaching environment (including complying with its responsibilities under the Safety, Health, and Welfare at Work Act 2005)
- To enable St. Michael's House to comply with requirements set down by the Revenue Commissioners, the HSE, the HPRA and any other governmental, statutory, and regulatory departments and Health related agencies
- For compliance with all legislation relevant to St. Michael's House
- Next of Kin and number in case of Emergency

b) Lawful Bases for processing:

- Consent
- Necessary for the execution of contractual obligations
- Statutory Obligations (e.g., payment of payroll taxes etc.)
- Vital Interest
- Necessary for Legal Obligation
- Public Tasks
- Legitimate Interest

c) Location and Security procedures of St. Michael's House:

- **Manual records** are kept locked and secured in all locations under the control of St Michael's House
- **Digital Records** are stored on servers which can only be accessed by password protected computers and laptops with adequate encryption and firewall software. Other electronic data is held on secure servers.
- **All mobile phones** are password protected and encrypted.

d) To prevent the loss of Personal Data while being transported to and from St Michael's House, employees working remotely may only have personal Data on laptops with adequate encryption and firewall software. Manual records are **Not** permitted to be brought home.

6. Management Data

Categories of Management data:

- Name, address, and contact details of each member of the Board of Management (including former members of the Board of Management) for the purpose of Companies Registration Office administration.
- Records in relation to appointments and resignations to and from the Board.
- Minutes of Board of Management meetings and correspondence to the Board, which may include references to individuals.

a) Purposes:

- To enable the Board of Management to operate in accordance with the Companies Act 2014 and other applicable legislation and to maintain a record of Board appointments and decisions
- To comply with all legal requirement

b) Lawful Bases for processing:

- Consent
- Necessary for the execution of contractual obligations
- Statutory Obligations (e.g., payment of payroll taxes etc.)
- Vital Interest
- Necessary for Legal Obligation
- Public Tasks
- Legitimate Interest

c) Location and Security procedures of St. Michael's House:

- **Manual Records** are kept locked and secured in all locations under the control of St Michael's House

Digital Records are stored on servers which can only be accessed by password protected computers and laptops with adequate encryption and firewall software. Other electronic data is held on secure servers.
All mobile phones are password protected and encrypted.

d) To prevent the loss of Personal Data while being transported to and from St Michael's House, employees working remotely may only have personal Data on laptops with adequate encryption and firewall software. Paper records are Not permitted to be brought home.

7. Other Records : Partner, Contractor, Third-Party Subcontractors, and Job Applicants

Categories of Personal data:

- St. Michael's House may hold some or all the following information about the above data subjects (some of whom may be self-employed individuals and/or Volunteers):
- Name
- Address
- Contact details and tenders
- PPS number
- VAT Registration
- Tax details
- Bank details and
- Amount paid
- Work history
- Qualifications
- Legal claims
- Next of Kin and number in case of Emergency

a) Purposes:

- This information is required for routine management and administration of St. Michael's House's financial affairs, including the payment of invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.

b) Lawful Bases for processing:

- Consent
- Necessary for the execution of contractual obligations
- Statutory Obligations (e.g., payment of payroll taxes etc.)
- Vital Interest
- Necessary for Legal Obligation
- Public Tasks
- Legitimate Interest

c) Location and Security procedures of St. Michael's House:

- **Manual records** are kept locked and secured in all locations under the control of St Michael's House
- **Digital Records** are stored on servers which can only be accessed by password

protected computers and laptops with adequate encryption and firewall software. Other electronic data is held on secure servers.

- **All mobile phones** are password protected and encrypted.

d) To prevent the loss of Personal Data while being transported to and from St Michael's House, employees working remotely may only have personal Data on laptops with adequate encryption and firewall software. Paper records are Not permitted to be brought home.

8. CCTV

St Michael's House processes CCTV recordings for the purpose of maintaining :-

a. Safety of St Michael's House Service Users, Staff, Visitors and Security of Premises.
b. Necessary to protect the vital interest of St Michael's House against Legal claims or Proceedings.
c. CCTV footage will not be held for longer than twelve (12) months, unless it is required for Legal purposes, in which case it may be held indefinitely.
d. St Michael's House CCTV footage inside and outside our premises will be provided to the Gardai.
e. CCTV footage will be kept safe and secure and will be protected against unauthorised access.
f. Gardai, Service users, Staff, Contractors, and Visitors to St Michael House may request to view CCTV footage on application in writing to the Data Protection Officer. Depending on the circumstance CCTV footage may be provided with images redacted, in picture format or complete video.
g. The Director of Human resources will have an Annual Data Protection Impact Assessment carried out.

9 Communications and Fundraising

St Michael's House also processes contact names, telephone numbers, addresses, email, social media identifiers, photographs, and videos for the purpose of Communications and Fundraising.

10. Responsibilities and roles under the General Data Protection Regulation

St Michael's House is a Data Controller under General Data Protection Regulations. St Michaels House determines the purpose for which, and how personal data is processed.

The Chief Executive Officer of St Michael's House and all those in managerial or supervisory roles throughout St Michael's House are responsible for developing and encouraging good information handling practices within St Michael's House. These responsibilities are set out in individual job descriptions.

11. <u>Data Protection Principles</u>

All processing of personal data must be conducted in accordance with the Data Protection Principles as set out in Article 5 of the GDPR. St. Michael's House's policies and procedures are designed to ensure compliance with these principles :-

12. Personal data must be processed lawfully, fairly, and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "Conditions for processing", for example consent.

Fairly – for processing to be fair, the data controller must make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

All draft communications are subject to Freedom of Information and General Data Protection Regulation. This relates to all draft records, minutes, reports, assessments etc. **The Final record** once agreed is the only record which should be retained. All recipients need to securely delete any soft or hard copies of previous drafts circulating including emails.

St. Michael's House's Privacy Notice Procedure is set out in our Privacy Policy Statement.
The specific information that must be provided to the data subject must, as a minimum, include:

a) the identity and the contact details of the controller and, if any, of the controller's representatives

b) where applicable, the contact details of the Data Protection Officer or the person responsible for Data Protection

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing

d) the period for which the personal data will be stored

e) the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected

f) the categories of personal data concerned

g) the recipients or categories of recipients of the personal data, where applicable

h) where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data

i) any further information necessary to guarantee fair processing.

13 Employee and Staff

Employees and staff are required to notify St. Michael's House of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of St. Michael's House to ensure that any notification regarding change of circumstances is recorded and acted upon. It is also the responsibility of the data subject to ensure that data held by St. Michael's House is accurate and up to date. The Data subject must update their information in writing or by email.

Personal data can only be collected for specific, explicit, and legitimate purpose Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of St. Michael's House's GDPR record of processing activities. Personal data must be adequate, relevant, and limited to what is necessary for processing.

14 Chief Executive Officers responsibility

The Chief Executive Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it. The Chief Executive Officer is responsible for ensuring that St Michael's House does not collect Information, that is not strictly necessary, for the purpose that it was obtained.

15 Data Collection Forms

All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and be approved by the Director of Human Resources of St. Michael's House.

16 Data Collection Methods reviewed Annually by Data Protection Officer

The Data Protection Officer will ensure on an Annual basis, that all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant, and not excessive.

17 Director of Human Resources and Accurate Records

Personal data must be accurate, secure, and kept up to date with every effort to erase or rectify without delay.

The Director of Human Resources is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate, secure, and up to date, considering the volume of data collected, the speed with which it might change and any other relevant factors. No data should be kept unless it is reasonable to assume that it is accurate. The Director of Human Resources will review the technical, physical, and procedural security controls in place for Data handling within St Michael's House and offsite employees working remotely at least once a year. This will include a Data Protection Impact Assessment on CCTV to include signage, use, issues relating to security, storage, retention,

access to and review of CCTV footage.

18 **On an Annual basis**, the Director of Human Resources **will review the retention** dates of all the personal data processed by St. Michael's House, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted and destroyed.

19 **Records Rectified** The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month of Subject Access Requests. This can be extended to a further two months for complex requests. If St. Michael's House decides not to comply with the request, the Data protection Officer must respond to the data subject to explain the reasoning and inform them of the right to complain to the supervisory authority and seek judicial remedy.

20 **Rectification of Records incorrectly sent out**
The Data Protection Officer is responsible for making appropriate arrangements, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

21. **Form of Personal Data**
Personal data must be kept in a form, such that, the data subject can be identified only for as long as is necessary for the purpose it was received.

22. **Data Held Beyond its Retention Period**
Where personal data is retained beyond the processing date, it will be / encrypted / pseudonymised as applicable to protect the identity of the data subject in the event of a data breach.

23. **Retention and Destruction**
Personal data will be retained in line with the Retention Policy and, once its retention date is passed, arrangement should be made for it to be securely destroyed. See **Appendix 1 Retention Policy**

24 **Approval of Chief Executive Officer to keep beyond Retention Period**
Approval must be sought from the Chief Executive Officer for specific approval for any Data Retention that exceeds the retention periods defined in the Retention Policy and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. The Chief Executive Officer will grant or refuse this request in writing.

25 **Director of Human Resources will carry out a RISK ASSESSMENT on security Annually.**
<u>Personal Data must be processed in a manner that ensures the appropriate security</u>
The Director of Human Resources will carry out an Annual Data Protection Risk Assessment, considering all the circumstances of St. Michael's House's controlling or processing operations. In determining appropriateness, the Director of Human Resources should also consider the extent of possible damage or loss that might be caused to individuals (e.g., staff, members, application users and contributors) if a security breach occurs, the effect of any

security breach on St Michael's House itself, and any likely reputational damage.

When assessing appropriate technical measures, the Director of Human Resources will consider the following :-
Password protection
Automatic locking of idle terminals (PCs / Laptops / Tablets)
Removal of access rights for USB and other memory media
Virus checking software and firewalls
Role-based access rights including those assigned to temporary or contract staff
Encryption of devices that leave St. Michael's House and its premises such as laptops
Security of local and wide area networks
Privacy enhancing technologies such as pseudonymisation and anonymisation.
Identifying appropriate international security standards relevant to St. Michael's House.
Acceptable use of Computer Resources

When assessing appropriate organisational measures, the Director of Human Resources will consider the following :-
- The appropriate training levels throughout St. Michael's House.
- Measures that consider the reliability of employees (such as references etc.).
- The inclusion of data protection in employment contracts.
- Identification of disciplinary action measures for data breaches.
- Monitoring of staff for compliance with relevant security standards.
- Physical access controls to electronic and paper-based records.
- Adoption of a clear desk policy.
- Storing of paper-based data in lockable fire-proof cabinets.
- Restricting the use of portable electronic devices outside of the company.
- Restricting the use of employee's own personal devices being used in the company.
- Adopting clear rules about passwords.
- Making regular backups of personal data and storing the media off-site.
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside of the EU/EEA.

These controls have been selected because of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

The GDPR includes provisions that promote accountability and governance. These complement the transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

St. Michael's House will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as Data Protection by design, DPIAs, Breach notification procedures and Incident response plans.

26. Data Subjects' Rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:-

To make subject access requests regarding the nature of information held and to whom it has been disclosed.

To prevent processing likely to cause damage or distress.

To prevent processing for purposes of direct marketing.

To be informed about the mechanics of automated decision-taking process that will significantly affect them.

To not have significant decision that will affect them, taken solely by automated process.

To sue for compensation if they suffer damage by any contravention of the GDPR.

To take action to rectify, block, erase (including the right to be forgotten) or destroy inaccurate data.

To request the supervisory authority to assess whether any provision of the GDPR has been contravened

To have personal data provided to them in a structured, commonly used, and machine-readable format, and the right to have that data transmitted to another controller.

To object to any automated profiling that is occurring without consent.

27. St. Michael's House ensures that Data Subjects may exercise these rights:

Data subjects may make **data access requests** as described in Subject Access Request Policy, (Appendix 11 to this policy) this also describes how St Michael's House will ensure that its response to the data access request complies with the requirements of the GDPR.

Data subjects have the right to complain to St. Michael's House related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints will be handled is contained in our Subject Access Request Policy, (Appendix 11 to this policy).

28. Consent

St. Michael's House understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed, and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

St Michael's House understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without information will not be a valid basis for processing.

There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication.

In the case of vulnerable non communicative individual's, the consent of "legal guardianship, be they parents or others" will be requested before processing their Data.

The Controller must be able to demonstrate that consent was obtained for the processing operation.

The processing of certain sensitive types of certain sensitive types of personal data, known as special categories of personal data, is prohibited, except for in limited circumstances, as set out in Article 9 GDPR. Such processing requires both a legal basis under Article 6 GDPR, as well as meeting one of the conditions of Article 9 (such as explicit consent or protection of vital Interests) which allow such data to be processed. From "Guidance on legal basis of Processing personal Data issued by the Data Protection Commission

Special Categories of Personal Data (also known as Sensitive Personal Data) – Which are highly relevant as they require higher level of protection. This is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

For sensitive data, explicit written consent of data subjects must be obtained **unless** an alternative legitimate basis for processing exists such as the exemption as detailed in Art. 9 (2) (d) where "processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association, or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;"

In most instances, consent to process personal and sensitive data is obtained by St Michael's House using standard consent documents from the legal guardianship, be they Parents, guardians or others.

St Michael's House provides services to children and processes children's data. The processing of the personal data of a child is lawful where the child is at least 16 years old, in line with the GDPR and the Data Protection Act 2018. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. St Michael's House will make all reasonable efforts to verify in such cases that consent is given or authorised by the legal guardians, be they Parents, guardians, or others.

29. Security of Data

All Employees and Staff are responsible for ensuring that any personal data, that St Michael's House collects, and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by St Michael's House to receive that information and has entered into a confidentiality agreement. St Michael's House operated a strict policy of confidentiality that is detailed in all contracts of Employment and service contracts. Staff members and Contractors may not disclose any information of a confidential nature relating to St Michael's House or its service users. This applies during and post-employment within the organisation. On termination of employment, all documentation, files, etc in a staff member's possession must be returned to St Michael's House

All personal data should be accessible only to those who are required to access it in the course of their work. All personal data should be treated with the highest security and must be kept **:-**

a. in a lockable room with controlled access; and/or
b. in a locked drawer or filing cabinet; and/or
c. if computerised, encrypted on servers and password protected on laptops and computers
d. or on (removable) computer media which are encrypted. All phones are password protected and encrypted.

Care must be taken to ensure that Personal Computer screens and terminals are not visible except to those authorised Employees and Staff of St Michael's House.
All Employees / Staff are required to enter into an Acceptable Use Agreement before they are given access to organisational information.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from company premises without explicit written authorisation. As soon as manual records are no longer required for day-to-day organisational support, they must be removed for secure archiving.

Personal data may only be deleted or disposed of in line with the **Retention Policy Appendix 1**. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed before disposal.

30. Data Breach Notification Procedure

In the event of a breach of security, potentially leading to the accidental or unlawful destruction, loss alteration, unauthorised disclosure of, or access to, personal data, the Data Protection Officer of St Michael's House must be notified immediately in line with the Data Breach Management Policy
The Communication Officer St Michael's House will also be notified.
(SEE APPENDIX 3 ON DATA BREACH MANAGEMENT POLICY).

The risk of individuals having their privacy impacted as a result of the personal data breached should be assessed by the Data Protection Officer. Notification to the Data Protection Commissioner Ireland and communication to the affected data subjects should be made if required.

31. Disclosure of Data

St Michaels House must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Gardai. All Employees and Staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of St Michael's House's operations.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer of St Michael's House with support from the administration staff.

32. Retention and Disposal of Data see also Appendix 1

St Michael's House shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

St Michael's House may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data is set out in **Appendix 1 Retention Policy** along with the criteria used to determine this period including any statutory obligations St Michael's House to retain the data. St Michael's House Data Retention and Data Disposal procedures will apply in all cases.

Personal data must be Disposed of Securely in accordance with the sixth principle of the GDPR processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of Data Subjects.

33. Data Transfer

All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects". The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply **: -**

An Adequacy Decision

The European Commission can and does assess third countries, a territory and, or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances, no authorisation is required. Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision. A list of countries that currently satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union. These include the UK and the USA and are listed on the website **:-**

http://ec.europa.eu/justice/data-protection/international-transfer/adequacy/index_en.htm

<u>Assessment of adequacy by the data controller</u>

In making an assessment of adequacy, the Irish based exporting controller should take account of the following factors **: -**

- the nature of the information being transferred.
- the country or territory of the origin, and final destination, of the information.
- how the information will be used and for how long.
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and the security measures that are to be taken as regards the Data in the overseas location.

Binding Corporate Rules
St Michael's House may adopt approved binding corporate rules for the transfer of data outside the EEA. This requires submission to the relevant supervisory authority for approval of the rules that St Michael's House is seeking to rely upon.

Model contract clauses
St Michael's House may adopt approved model contract clauses for the transfer of data outside of the EEA. If St Michael's House adopts the model contract clauses approved by the relevant supervisory authority, an associated Transfer Impact Assessment must be carried out and appropriate safeguards applied.

Exceptions
In the absence of an adequacy decision, binding corporate rules and / or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions: -

The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.

The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.
The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.
The transfer is necessary for important reasons of public interest.
The transfer is necessary for the establishment, exercise, or defence of legal claims; and/or the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

Data relating to service users:

The lawful basis for the transfer of service user files is underpinned by the Health Acts 1947-2020 & under GDPR 6.1(e) [public interest] & 9.2 (h) section 52 of the Data Protection Act 2018 where the processing "is undertaken by or under the responsibility of (a) a health practitioner (as defined in the Health Identifiers Act 2014) or (b) a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which would exist if that person were a health practitioner" [provision of care].

The information that we collect about you may include details such as:

- Name, address, telephone, email, date of birth and next of kin
- Any contact we have had with you through appointments and hospital attendances
- Details and records of treatment and care, notes and reports about your health, including any allergies or health conditions
- Results of diagnostic tests, e.g. x-rays, scans, blood tests
- Financial and health insurance information
- Other relevant information from people who care for you and know you well, e.g. health professionals, relatives and carers.

- We may also collect other information about you, such as your sexuality, race or ethnic origin, religious or other beliefs, and whether you have a disability or require any additional support with appointments (like an interpreter or advocate).
- CCTV and security information.

Why do St Michael House collect information about you ?
To make sure you get the best care, doctors, nurses and the team of healthcare staff caring for you keep records about your health and any care or treatment you may receive from us. It is important for us to have a complete picture as this information enables us to provide the right care to meet your individual needs.

How we store your personal data
Your information is collected in a number of different ways. This might be from a referral made by your GP or another healthcare professional you have seen, or perhaps directly from you - in person, over the telephone or on a form you have completed. There may also be times when information is collected from your relatives or next of kin e.g. if you are taken to our emergency department (A&E) but you are very unwell and unable communicate. During your treatment health specific data will be collected by the doctors, nurses and healthcare staff taking care of you and will be held in your patient chart (This can be paper and/or electronic).

How we store your personal data ?
Under GDPR, strict principles govern our use of personal data and our duty to ensure it is kept safe and secure. Your data may be stored within electronic or paper records, or a combination of both. All our records have restricted access controls, so that only those individuals who have a need to know the information can get access. This might be through the use of computer passwords, audit trails and physical safeguards e.g. security controlled access.

How we use your information and why this is important ?
We use your information **to manage and deliver your care (Direct Care)** to ensure that:

- The right decisions are made about your care
- Your treatment is safe and effective; and
- We can coordinate with other organisations that may be involved in your care.

This is important because having accurate and up-to-date information will assist us in providing you with the best possible care.

In addition to using the data to provide for your care, this data is also routinely used **to improve services and plan for the future (Indirect Care)**, therefore, your data may be used in:

- Evaluating and improving patient safety
- Reviewing the care provided to ensure it is of the highest standard possible, improving individual diagnosis and care. This can be carried out by multiple quality improvement methods e.g. clinical audit.
- Training healthcare professionals
- Ensuring that our services can be planned to meet the future demand. E.g. analysing peak times, staffing levels and average length of stay, projected demand by disease/condition.
- Preparing statistics on hospital performance and monitoring how we spend public money

- Supporting the health of the general public e.g. Influenza, winter vomiting bug.

- **The activities listed above are part of normal delivery of care and under GDPR your consent is not required**. However, we recognise our duty to always keep your data secure and confidential and where appropriate we de-identify your data when using it for improvement. Using the data to understand and develop new treatments and techniques (Research). Research in healthcare is vital in helping develop understanding about health risks and causes to develop new treatments. It is usual for patient information to be used for research. **Your consent will be sought prior to being asked to participate in a research study** or to have your personal data used in a research study. In some circumstances, consent exemptions may be granted by the Health Research Board Consent Declaration Committee (HRBCDC). You will not be identified in any published results without your prior agreement.

34. Records of Processing / Data Inventory

St Michael's House has clear established records of processing activities and data inventory as part of its approach to address and mitigate risks and opportunities throughout its GDPR compliance project.
These are listed as follows :-

St Michael's House's Records of Processing determines:

- business processes that use personal data
- source of personal data
- volume of data subjects
- description of each item of personal data
- processing activity
- maintains the inventory of data categories of personal data processed
- documents the purpose(s) for which each category of personal data is used
- recipients, and potential recipients, of the personal data
- the role of St. Michael's House throughout the data flow
- key systems and repositories
- any data transfers; and
- all retention and disposal requirements.

35. Risk / Impact Assessments Data Protection Impact Assessments (DPIAs)

St Michael's House is aware of any risks associated with the processing of particular types of personal data.

St Michael's House assesses the level of risk to individuals associated with the processing, of their personal data. Data Protection Impact Assessments (DPIAs) are carried out in relation to the processing of personal data by St Michael's House, and in relation to processing undertaken by other organisations on behalf of St Michael's House where necessary. St Michael's House shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

Where a type of processing, in particular using new technologies and, taking into account the nature, scope, context, and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, St Michael's House shall,

prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

Where, as a result of a DPIA it is clear that St Michael's House is about to commence processing of personal data that could cause damage and /or distress to the data subjects, the decision as to whether or not St Michael's House may proceed must be escalated for review to the Data Protection Officer.

The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority. Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to St Michael's House's documented risk acceptance criteria and the requirements of the Data Protection Act and the GDPR.

36. Document Owner and Approval

The Chief Executive Officer is the owner of this document and is responsible for ensuring that this policy is reviewed in line with the review requirements for the GDPR. A current version of this document is available to all members of staff on the Notice Board.

This policy and appendices were approved by the Chief Executive Officer of St. Michael's House on the 01 / 01 / 2024 and is issued on a version control basis under the Chief Executive Officers signature.

Signature:  Date: 07.02.2024

37

APPENDIX ONE

Policy for the Retention of Records.

St. Michael's House

Policy for the Retention of Records.

POLICY FOR RETENTION OF RECORDS

38. Introduction

This policy applies to all records, irrespective of format, held by, under the control of, or in the possession of St. Michael's House. It applies to all personnel (including contractors) in all service areas and all locations. It applies to all aspects of data processing including record creation, maintenance, and disposal. It includes all applications used to create records including, without being limited to, e-mail, database applications and websites. All information, written and electronic, created or received by staff of St. Michael's House preserved in the form of a record, is covered by this policy.

39. Ownership of Records

All records, irrespective of format, created or received by personnel, in the course of their work on behalf of St. Michael's House, are the property of St. Michael's House and are subject to its overall control. Individual staff do not own the records. But have responsibility for managing records according to this policy.

40. Purpose and Objectives

The purpose of this policy is to:

- Support records management within St. Michael's House.
- Support the organisation's administrative and operational requirements, including adherence to the organisation's policies and compliance with relevant legislation.
- Ensure preservation of appropriate records.
- Promote day-to-day efficiency and good office management.
- Ensure timely destruction of records that no longer need to be retained.

This policy applies equally to records created and preserved in electronic and paper formats.

41. Records Management

Records management is the application of procedures to the creation, maintenance, use and disposal of records in accordance with approved procedures. This includes:

- Records classification
- Management of filing systems
- Retention scheduling
- Administration of inactive records storage
- Appropriate destruction of record

42 Responsibilities of St. Michael's House Personnel

The Chief Executive Officer (CEO) has overall responsibility for Records management in the organisation. The CEO's office is responsible for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this as it will ensure appropriate, accurate information is available as required. St. Michael's House has a responsibility for ensuring that at a corporate level it meets its legal requirement along with the internal and external governance requirements.

The responsibility for local records management is devolved to the relevant Directors, Administration Managers, Service Managers, Heads of Departments,

and Persons in Charge. The business functions of St. Michael's House have overall responsibly for the management of records generated by their activities, which is to ensure that records controlled within their area, are managed in a way which meets the organisations records and retention policy.

All Staff, clinical, administrative, front line, Interns, trainees and students on placements who create, receive, and use records have records management responsibilities. In particular, all staff must ensure that that they keep appropriate records of their work in the organisation and manage these records in keeping with this policy.

This policy applies to all service areas and all activities. Each person is responsible for their own records. Where records are used by more than one person or service area agreement about which person or team has primary responsibility for management of the records should be established between the relevant staff members.

The confidentiality of information within records must be always safeguarded. It is the responsibility of each team to ensure that the appropriate security measures are observed for maintaining records containing confidential information. Particular attention must be given to the commitments (if any) given to the data subject when personal data is acquired, irrespective of the legal basis on which it was acquired and processed. The use, retention and destruction of personal information must align to the representations made by St. Michael's House at that critical juncture.

Once records have been retained for the time stipulated in the HSE Retention Schedule see also Appendix One, they must be destroyed in accordance with the schedule. When scheduled for destruction, records must be disposed in the manner indicated in the Retention Schedule. **A register of the destruction of records should be maintained. In the case of third-party destruction, a certificate confirming destruction should be received and retained as proof of destruction. See also para 52.**

43. Definition of a Record

Records are documents and data in all formats, which are created / received and maintained as evidence of business completed or as a source of knowledge and which must be retained for as long as required to meet the legal, administrative, financial, or operational needs of St. Michael's House.

44. Forms of Records

Records may exist in a variety of physical forms including:-
Paper documents
Electronic records (computer files, databases, spreadsheet files, emails, CCTV footage, electronic data on any media) and other machine-readable records
Books, maps, plans, drawings, photographs
Copies of original records

45. Electronic Records

The nature of electronic records requires that consideration be given to security, authenticity, accessibility, version control, back-up of records and the disposal of such records.

St. Michael's House personnel must employ the following good housekeeping practices in the management of electronic records **:**

- Appropriate naming of files and folders
- Backup of appropriate files on a regular basis
- Delete records regularly in accordance with the HSE and St Michaels House Retention Schedule
- Restrict access to record systems as appropriate (use of passwords, timed lock out of PCs etc.); and

In the case of electronic records where the computer (or similar device) is owned by St. Michael's House, each person is expected to agree backup procedures with St. Michael's House. No electronic records are to be kept on computers (or similar devices) not maintained by St. Michael's House.

46. Email

Email has become a widely used and effective method of communication in the workplace. Email carries the same legal status as other forms of communication, and all personal data needs to be handled within the principals of GDPR and are also subject to the Freedom of Information Acts.

- **Every staff member has an @SMH email account. Only @smh.ie emails addresses should be used for all SMH email communications.** The use of external email addresses such as Gmail, yahoo, outlook etc for internal SMH communications **is prohibited**
- No personal information should be contained in the body of an email. Personal data should be held in an attachment. Always ensure that confidential or personal information is sent to the correct recipient and only sent to relevant staff members for a given function to be carried out.
- St Michael's house uses TLS encryption on all mails entering and leaving the St Michael's network domain.
- No personal information about a Service User should be sent by email, to or from, a staff member's private email address.
- Emails relating to service delivery should be written in clear concise language avoiding use of abbreviations or informal comment.
- When emails are being sent to a number of outside recipients the BCC will be used instead of CC

47. Draft records

St. Michael's House has developed a specific protocol around draft records relative to the FOI and the GDPR. The protocol that applies is that once the final draft of a document is agreed upon, all parties should securely delete any hard or soft copies of previous drafts. The final record is the only one which should be retained and securely stored by St Michael's House staff.

48. Devices

Personal information about service users may only be stored, replicated, or transferred to St Michaels House electronic devices that have been encrypted by

the organisation. Such devices include USB keys, PDAs, Mobile Phones, Multi-media players or other mobile external devices. Under no circumstances can service user information be stored on personal computers, personal phones, or other personal electronic devices.

49. Images

Digital, photographic, or video images should only be recorded, stored, or used with the explicit consent of the employee, service user or their family and from the relevant line manager.

Photographs or images for clinical or medical purposes should be specific to the nature of the pertaining issue or purpose (e.g., pressure sore, rash, bruises etc.). Images should be deleted from the camera/ device at the earliest opportunity and should be stored in the clinic file. See St Michael's House Clinical Photography Guidelines on the intranet for more information

Note this does not apply to CCTV footage which is covered under a different paragraph in this policy.

St Michael House values the use of visuals as one way to make information more accessible to the people we support. To avoid Data Breaches all staff members are reminded about the importance of using only authorised photos and images in our documents, both internal and external.

50. Management and Retention of Records

Records should be retained for as long as they are required to meet the legal, administrative, financial, and operational requirements of St. Michael's House during which time, they should be filed appropriately. Following a period, St Michael's House will in accordance with HSE and St Michaels House retention policy, list the records and then destroy the records. A copy of the records destroyed will be sent to the DPO. The DPO will retain the list of destroyed records.

St. Michael's House holds the following classes of records:

- Records of children supported by St. Michael's House
- Records of adults supported by St. Michael's House
- Human resource management records
- Financial records, insurance and legal
- Governance records

St. Michael's House's retention schedule details the records held under each classification, the retention period, and the final disposition method.

51. Legislation / Regulation / Standards

St Michaels House complies with all current legislation, regulation, and standards.

St Michael's House are bound by the Freedom of Information Act 2014 and the General Data Protection Regulation 2018 to maintain and make available records, to which people who use our services and staff, have a right of access. It also adopts but is not limited to the HSE Standards and Record Retention Periods Health Service Policy 2013.
In addition to the St Michael's House policies and procedures, administrative and operational requirements and general best practice, the Retention Schedule is based on a determination of legal retention requirements as defined in relevant legislation including: -

- Companies Acts 1963-2014
- Income Tax Act 2007
- Health and Safety at Work etc. Act 1974, Safety, Health and Welfare at Work Act 2005, Safety, Health, and Welfare at Work (General Application) Regulations 2007 and Protection of Employees (Part time Work)Act 2001
- Freedom of Information Act 2014
- Insolvency Act 1986
- Data Protection Acts 1984 to 2018
- Equality Act 2010
- Communications Regulation Acts 2002 to 2016
- Terms of Employment (information) Act 1994
- Organisation of Working Time Act 1997
- And any other legislation enacted that require St Michael's House to retain records

52. Disposal of Records

All records created and received must be disposed of in a manner that safeguards confidentiality and privacy of the information they contain. All records that are created and recorded by the organisation that are permanently preserved must remain accessible to authorised staff where required. The chosen method of final disposition for each record should be documented in the Retention Schedule.
A register of records destroyed should be maintained as proof that the record no longer exists. The register should show: -

a) Persons' name
b) Date of birth
c) Address
d) Name of the file
e) File/record number
f) Former location of file
g) Date of destruction
h) Who gave the authority to destroy the records & their signature of approval for destruction

53. Confidential records

It is vital that the process of record disposal safeguards and maintains the confidentiality of the records. This can be achieved internally or via an approved records shredding

contractor, but it is the responsibility of the Chief Executive Officer to be satisfied that the methods used provide adequate safeguards against accidental loss or disclosure of the records.

Any record containing personal identifiable information such as name, address, date of birth, PPS Number, employee number, or medical record is deemed confidential. Other records may also be confidential if they contain information about the organisation's business or finances. Examples of confidential documents include financial records, payroll records, personnel files, legal documents, or medical records.

Only some documents are confidential and should be disposed in confidential paper bins or security bags. Alternative paper recycling options should be provided for non-confidential paper / magazines. If shredding off-site, confidential waste should be secure until uplift by the shredding contractor.

Confidential waste bags/wheelie bins should be exchanged by the shredding contractor, and shredded off-site at an agreed location. If confidential waste is transported off site, the contractor must ensure that documents are destroyed and never read by members by members of the public.

54. Destructions of Digital Media

It is essential when disposing of hard drives, tapes, CDs, memory keys, mobile phones, credit cards, fax machines, printers, x-rays films and any other media containing data that a reliable, secure, traceable, and certifiable destruction method is used. There are various companies who provide these services.

55. Retention Schedule

General class of record	Retention period	Final disposition	Source of guidance
Records created under Childcare Acts	Hold in perpetuity	Not applicable	Section 5 HSE Records Retention Periods Health Service Policy 2013
Wards of Court	Hold in perpetuity – Childcare (Placement of Children in Foster care Regulations 1995)		HSE Records Retention Periods Health Service Policy 2013
Case records & registers: Children in residential care	Hold in perpetuity – Childcare (Placement of Children in Foster care Regulations 1995)	Not applicable	Section 5 HSE Records Retention Periods Health Service Policy 2013
Social work – Records created under childcare legislation, housing, welfare etc.	Hold in perpetuity – Childcare (Placement of Children in Foster care Regulations 1995)	Not applicable	Section 5 HSE Records Retention Periods Health Service Policy 2013
Social work – Records created under childcare legislation, housing, welfare etc.	Hold in perpetuity – Childcare (Placement of Children in Foster care Regulations 1995)	Not applicable	Section 5 HSE Records Retention Periods Health Service Policy 2013
Social work records of children supported by services	Retain indefinitely during the lifetime of the person, and for 8 years after death. Note Records created under the Childcare legislation - hold in perpetuity.	Destroy under confidential conditions	Section 5 HSE Records Retention Periods Health Service Policy 2013

Records of Adults General class of record	Retention period	Final disposition	Source of guidance
Records of people currently supported by services	Retain indefinitely during the lifetime of the person, and for 8 years after death	Destroy under confidential conditions however if serious untoward issues arise keep for up to 30 years after death	HCR42 HSE Records Retention Periods Health Service Policy 2013
Records of people no longer availing of services	Retain for 20 years from date of last entry in the records and retain core details e.g. name, address, date of birth, date of admission, date of discharge and birth cert in perpetuity.	Destroy under confidential conditions or archive as appropriate	HCR42 HSE Records Retention Periods Health Service Policy 2013
Records of applicants for services who are not admitted or not entered on a waiting list	Retain for 10 years	Destroy under confidential conditions	HSE Records Retention Periods Health Service Policy 2013
Psychology records of people supported by services	Retain indefinitely during the lifetime of the person, and for 8 years after death	Destroy under confidential conditions	HCR48 HSE Records Retention Periods Health Service Policy 2013
Social work records of adults supported by services	Retain indefinitely during the lifetime of the person, and for 8 years after death	Destroy under confidential conditions	HCR52 HSE Records Retention Periods Health Service Policy 2013
Speech & language therapy records	Retain indefinitely during the lifetime of the person, and for 8 years after death	Destroy under confidential conditions	HCR53 HSE Records Retention Periods Health Service Policy 2013
Clinical audit records	5 years	Destroy under confidential conditions	HCR11 HSE Records Retention Periods Health Service Policy 2013
Photographs (where the photo relates to a particular patient it should be treated as part of the healthcare record).	Retain indefinitely during the lifetime of the person, and for 8 years after death	Destroy under confidential conditions	HCR43 HSE Records Retention Periods Health Service Policy 2013

Healthcare records (excluding records not specified elsewhere in the schedule)	8 years after conclusion of treatment or death	Destroy under confidential conditions	HCR23 HSE Records Retention Periods Health Service Policy 2013
'Serious untoward incident' records	30 years after death	Destroy under confidential conditions	HCR24 HSE Records Retention Periods Health Service Policy 2013
Records of Destruction of Individual Healthcare records (case notes) and other health related records contained in this retention schedule (in manual or computer format)	Permanently		HCR50 HSE Records Retention Periods Health Service Policy 2013
Admission books (where they exist in paper format)	8 years after last entry	Likely to have archival value. Contact the National Archives (RADD)	HCR3 HSE Records Retention Periods Health Service Policy 2013
Discharge books (where they exist in paper format)	8 years after last entry	Likely to have archival value. Contact the National Archives (RADD)	HCR18 HSE Records Retention Periods Health Service Policy 213

General class of record held	Retention period	Final disposition	Source of guidance
Annual leave request records	3 years	Destroy under confidential conditions	Organisation of The Working Time Act 1997 stipulate keeping these records for 3 years
Recruitment competition files	2 years	Destroy under confidential conditions	See Employment Equality Act 1998-2015. The legal requirement is to keep competition files for a minimum of 6 months with a further 6 months necessary if a case is brought against the employer under the Equality Act. A period of 2 years more than adequately meets the legislative requirements and provides a reasonable period of time to provide reasons for Decisions under Section 10 of the FOI Act 2014
Personnel file	(1) Human resources shall ensure that the records set out in Schedules 2, 3 and 4 are made available to a designated centre for inspection by the Chief Inspector. (2) Records kept in accordance with this section and set out in Schedule 2 shall be retained for a period of not less than 7 years after the staff member has ceased to be employed in the designated centre concerned. And / or depending on your practice HR retain for duration of employment forward to Pensions on retirement. Hold for 7 years after death of pensioner	Destroy under confidential conditions	Health Act Regulation 2013 Part 6 HSE Records Retention Policy 2013

Garda vetting application forms	Original application forms go to and are held by the Garda Vetting Unit (NRS) only. No application forms should be held at local level. Confirmation notices are held at local level. 7 years	Destroy under confidential conditions	Health Act Regulation 2013 Part 6 HSE Records Retention Policy 2013
Garda vetting	Disclosures 1 year (keep number & date)	Destroy under confidential conditions	6.0 HSE Records Retention Policy 2013
Garda vetting confirmation notices	1 year	Destroy under confidential conditions	
Pensioner file	7 years after death of pensioner	Destroy under confidential conditions	6.0 HSE Records Retention Policy 2013
Industrial relations/Trade Union negotiations	Retain indefinitely	Archive	6.0 HSE Records Retention Policy 2013
Pay & conditions (exceptions)	Retain indefinitely	Archive	6.0 HSE Records Retention Policy 2013
Employer/Industrial relation case files	7 years from completion of the case	Destroy under confidential conditions	6.0 HSE Records Retention Policy 2013
Occupational health records – pre-employment medical reports	Retain indefinitely	Archive	Appendix 1 Human Resource Detail HSE Health Service Policy 2013 Record Retention Periods
Unsolicited applications for jobs	1 year	Destroy by shredding	
Student work placement records	Original 7 years	Destroy by shredding	
Training Course Content and Revision, Annual Programme of Courses and Training, and Attendance lists for Mandatory Training Information and published material on external training courses and 3rd level courses	Retain one set indefinitely 3 years after information has been superseded	Archive Destroy by shredding	

Annual Leave Request Records include, sick leave record including certificates, career break applications and correspondence, special leave, jury service leave, compassionate leave record and superannuation. (The Organisation of Working Time Act 1977)	Sick certificates - 3 years. (Organisation of Working Time (Records) (Prescribed Forms and Exemptions) Regulations, 2001, S.I. 473/2001.) Other absence records 8 years (Parental Leave Acts 1998 and 2006; Carer's Leave Act 2001) Records required for calculation of pension - forward to Pensions on retirement. Hold for 7 years after death of pensioner	Destroy under confidential conditions	Appendix 1 Human Resource Detail HSE Health Service Policy 2013 Record Retention Periods
Duty rosters & staff attendance records	Hold for 6 years after the year to which they relate	Destroy under confidential conditions	9.0 HSE Health Service Policy 2013 Record Retention Periods
Pension files – include information such as the refund file, preserved benefit statements, and temporary service files, Calculations and final awards, contributions paid, reports and adjustments, copy of birth certificate/passport, unpaid absences records, payroll adjustments letters for unpaid sick leave, parent leave, unpaid maternity leave, career break, pensionable service, pre-entry service, purchased service, records of refunds, and transferred service certificates of service letters.	Retain for 7 years after death of pensioner	Archive	Appendix 1 Human Resource Detail HSE Health Service Policy 2013 Record Retention Periods

Allegations & complaints	If complaint unfounded hold in sealed envelope on file for 7 years and then destroy. Where the matter involved criminal activity, these records should be retained indefinitely	Destroy under confidential conditions Archive	Appendix 1 Human Resource Detail HSE Health Service Policy 2013 Record Retention Periods
Complaint files FOI requests Data Protection requests Ombudsman / Information Commissioner requests	It is recommended that a retention period of a maximum of 7 years applies to files created under; the FOI Acts, the Data Protection Acts and following engagement with the Ombudsman, the Ombudsman for Children, the Information Commissioner *Where possible electronic copies of files should be created, therefore avoiding the need to keep the paper copies for the 7-year period other than: - those files created under the Child Care Act 1991 which shall be held in perpetuity -cases still ongoing - cases that involved legal action -cases that create a precedent (It is recommended that a similar policy is applied to non-personal records of this nature)	Destroy under confidential conditions	8.0 HSE Health Service Policy 2013 Record Retention Periods

Litigation dossiers and records relating to any form of litigation e.g.HR investigative files	If under investigation or if litigation is likely, files must be held in original form indefinitely	Archive	9.0 HSE Health Service Policy 2013 Record Retention Periods
Volunteer Records including those applicants who have been judged to be unsatisfactory.	10 years after volunteer leaves	Destroy under confidential conditions	Volunteering Ireland guidelines for organisations
Staff diaries	5 years	Destroy by shredding	7.0 HSE Health Service Policy 2013 Record Retention Periods
Service Diaries: (Service diaries that include information relating to individuals care) House Maintenance Log (information relating to household maintenance only)	Retain indefinitely 3 years	Archive Destroy by confidential shredding	
External Quality Control Records Internal Quality Control records	2 years 10 years	Destroy by confidential shredding	4.0 HSE Health Service Policy 2013 Record Retention Periods
Health & Safety – accident statistics	Retain indefinitely	Archive	Safety, Health & Welfare Act 2005
Health & Safety – fire drill records	Retain original indefinitely. Destroy copies after 2 years	Archive	Safety, Health & Welfare Act 2005
Fire equipment cert copies – service areas	6 years from date equipment is decommissioned	Destroy under confidential conditions	Safety, Health & Welfare Act 2005
Fire registers	Retain original indefinitely	Archive	Safety, Health & Welfare Act 2005
Health & Safety - Audits, Codes of Practice, Insurance correspondence, Hazard/Incident Report Forms, Authority Correspondence, records of meetings, Manual Handling Risk Assessment	Retain original indefinitely	Archive	Safety, Health & Welfare Act 2005

Checklists, Pregnant Employee Assessment Forms, Risk Assessment reports, Safety Audits, Safety inspections, Safety Statements, and Safety Training Records.			
Health & Safety – safety manuals & safety policies	Retain for 2 years after they have been superseded	Destroy by shredding	Safety, Health & Welfare Act 2005

Financial records,	insurance & legal		
General class of record held	Retention period	Final disposition	Source of guidance
Annual financial statements	Retain indefinitely	Archive	HSE Retention of Financial Records NFR-08
Audit reports	6 years	Destroy by shredding	HSE Retention of Financial Records NFR-08
Bank reconciliation	Monthly reconciliations – 1 year Yearend reconciliations – 6 years	Destroy by shredding	HSE Retention of Financial Records NFR-08
Bank statements	Original – 10 years Copies – 2 years	Destroy by shredding	HSE Retention of Financial Records NFR-08
Purchasing ledger - Invoices - Payments	Original – 6 years Copies – 2 years	Destroy by shredding	HSE Retention of Financial Records NFR-08
Cancelled cheques	6 years	Destroy by shredding	HSE Retention of Financial Records NFR-08
Capital projects – Invoices/Quotations/Tenders	Retain for 12 years from end of project		HSE Retention of Financial Records NFR-08
Circulars F. Team	Retain indefinitely	Archive	HSE Retention of Financial Records NFR-08
Contract/Contract Management files	Hold for 2 years after expiry of contract	Destroy by shredding	HSE Retention of Financial Records NFR-08
Control account reports	6 years	Destroy by shredding	
Dept of Health & Children circulars & correspondence	Retain indefinitely	Archive	HSE Retention of Financial Records NFR-08
Depreciation schedules	6 years	Destroy by shredding	HSE Retention of Financial Records NFR-08

Management account reports	1 year - Service Areas Year End Report - 6 years at Head Office	Destroy by shredding	HSE Retention of Financial Records NFR-08
General correspondence on financial administration	Retain for 12 years	Destroy by shredding	HSE Retention of Financial Records NFR-08
House accounts – Receipts/Invoices/Reports	Hold for 6 years at head office	Destroy by shredding	
Internal financial policies	Hold for 6 years at head office	Archive	HSE Retention of Financial Records NFR-08
Invitation to tender documents	Hold for 2 years after end of contract	Destroy by shredding	HSE Retention of Financial Records NFR-08
Journals	6 years	Destroy by shredding	
Paid cheques/copy/cheques/ electronic transfers	6 years	Destroy by shredding	HSE Retention of Financial Records NFR-08
Payment authorisation books	Hold for 2 years	Destroy by shredding	
Petty cash	Original - 6 years (Head Office) Copies – 2 years	Destroy by shredding	
Property accounts/fund accounts of people supported by services	Hold indefinitely or for 6 years after death	Destroy by shredding	HSE Retention of Financial Records NFR-08
Purchase order books	Original - 6 years, copies - 2 years	Destroy by shredding	HSE Retention of Financial Records NFR-08
Receipt books	Original - 6 years, copies - 2 years	Destroy by shredding	HSE Retention of Financial Records NFR-08
Sales ledger Invoices Receipts	Original - 6 years, copies - 2 years	Destroy by shredding	HSE Retention of Financial Records NFR-08
Supplier proposals	Hold for 2 years after award of contract	Destroy by shredding	HSE Retention of Financial Records NFR-08
Tax clearance certs	Hold until superseded by a more recent Tax Clearance Cert or for 6 years from last supplier interaction	Destroy by shredding	HSE Retention of Financial Records NFR-08
Tenders (successful)	Tender period plus 6 years	Destroy by shredding	
Tenders (unsuccessful)	6 years	Destroy by shredding	

Travel claims	Original - 6 years, copies - 2 years	Destroy by shredding	HSE Retention of Financial Records NFR-08
Building & engineering works	Retain indefinitely	Archive	
Deeds & titles of properties/assets	Retain indefinitely	Archive	HSE Retention of Financial Records NFR-08
Equipment – inspection reports	Lifetime of installation. If there is any measurable risk of a liability in respect of installations beyond their operational lives, the records should be retained indefinitely	Destroy by shredding	PATH5 HSE Health Service Policy 2013 Record Retention Periods
Equipment – records of non-fixed equipment, including specification, test records, maintenance records and logs	Lifetime of equipment. If there is any measurable risk of a liability in respect of equipment beyond their operational lives, the records should be retained indefinitely	Destroy by shredding	PATH 5 HSE Health Service Policy 2013 Record Retention Periods
Lease agreements	Hold for 6 years after expiration	Destroy by shredding	HSE Retention of Financial Records NFR-08
Manuals (operating)	Lifetime of equipment	Destroy by shredding	
Plans - building (as built)	Lifetime of building	Archive	
Properties – sale & purchase records	Retain indefinitely	Archive	HSE Retention of Financial Records NFR-08
Property register	Retain indefinitely	Archive	HSE Retention of Financial Records NFR-08
Vehicle Records: Drivers' logbooks, Vehicle mileage records etc.	5 years unless litigation ensues	Destroy by shredding	
Vehicle Records: Registration records	5 years unless litigation ensues	Destroy by shredding	

Accident reports	Original – indefinitely Copies – 2 years	Archive	HSE Retention of Financial Records NFR-08
Staff driving licences	5 years unless litigation ensues	Destroy by shredding	
Copies of staff motor insurance policies	5 years unless litigation ensues	Destroy by shredding	
Incident reports	Original – indefinitely Copies – 2 years	Destroy by shredding	
Insurance certificates	5 years unless litigation ensues	Destroy by shredding	
Insurance claim documents	Retain indefinitely	Archive	HSE Retention of Financial Records NFR-08
Insurance policies – motor vehicles	5 years unless litigation ensues	Destroy by shredding	
Insurance policies –property owned - property leased	Retain indefinitely	Archive	HSE Retention of Financial Records NFR-08
Listings/payslips	Retain indefinitely	Archive	
P35 reports	Retain indefinitely	Archive	
P60 reports	Retain indefinitely	Archive	
Payroll creditors – VHI, AVC, INO	Retain indefinitely	Archive	
Payroll month-end reports	Retain indefinitely	Archive	
Payroll salary adjustments	Retain indefinitely	Archive	
Payroll union contributions	Retain indefinitely	Archive	
Payslips	Retain indefinitely	Archive	
PIMS/SIMS year-end reports	Retain indefinitely	Archive	
Salary scales/national wage agreements	Retain indefinitely	Archive	6.0 HSE Health Service Policy 2013 Record Retention Periods
Staff Complement File/Census Returns/Employment Controls	Retain indefinitely	Archive	6.0 HSE Health Service Policy 2013 Record Retention Periods
Staff personnel files	Retain until 6 years after death or death of beneficiary and/or qualifying dependent	Archive	
Tax credit certs	Retain indefinitely	Archive	

Weekly timesheets	6 weeks after the year to which they relate	Destroy under confidential conditions	Organisation of Working Time Act 1997 stipulates keeping these records for 3 years
Records related to any litigation	As advised by the organisation's legal advisor. All records to be reviewed. Normal review 10 years after the file is closed	Destroy under confidential conditions	HCR49 HSE Health Service Policy 2013 Record Retention Periods
Legal opinion reports	Retain indefinitely	Archive	
Company seal	Keep for 6 years after the company is dissolved	Destroy under Confidential & Secure Conditions or Secure Archive	Company Act 2014
Company Documents e.g. Articles & Memorandum, / Company Charter, Legal documents of incorporation etc.	Keep for 6 years after the company is dissolved	Destroy under Confidential Conditions or Archive	Company Act 2014
Board minutes of meetings and associated papers, agendas, and reports. Written Resolutions Published Statutory Notices Copy of Company Letterhead Board sub-committee minutes of meetings and associated papers, agendas, and reports	Keep for 6 years after the company is dissolved	Destroy under Confidential Conditions or Archive	Company Act 2014
Copies of Board Compliance documentation including but not limited to: Governance Checklists, Conflict of interest statements. Beneficial Ownership Registration (on RBO portal) List of Directors for rotation purposes. Board Expenses Sheets Various Registers – Register of members Register of Directors & secretaries Register of Directors & Secretary's interests. Register of debenture holders Register of Company Assets.	Keep for 6 years after the company is dissolved	Destroy under Confidential Conditions or Archive	Company Act 2014 Charities Act 2009 Ethics & Standards in Public Office Money Laundering Act 2018
Copies of Board Handbooks, Codes of Conduct, Policies & Procedures for operation of the Board.	Keep for 6 years after the company is dissolved	Destroy under Confidential & Secure Conditions or Secure Archive	Company Act 2014

Reports to State Bodies from the Board e.g. copy of returns to the CRO e.g. B10 Forms, CRA e.g. Trustee Declaration Forms. Annual Reports & Strategic Plans.	Keep for 6 years after the company is dissolved	Destroy under Confidential & Secure Conditions or Secure Archive	Company Act 2014
Employers' liability insurance policy and schedule.	40 years from the date the company was dissolved	Destroy under Confidential Conditions or Archive as appropriate	Company Act 2014

56

APPENDIX TWO

Subject Access Request .

St. Michael's House

Subject Access Request

SUBJECT ACCESS REQUEST POLICY

57. Data Subject Rights

St. Michael's House's employees may collect, store or process personal data in the course of their employment with the organisation. Every employee has responsibilities under data protection legislation to protect the rights of the individuals whose personal data St. Michael's House obtains, stores or processes ("data subjects").

Data Subjects for whom St. Michael's House obtains personal data have the following rights**:-**

- To have their personal data obtained and processed fairly.
- To have personal data kept securely and not illegitimately disclosed to others.
- To be informed of the identity of the Data Controller and of the purpose for which the information is held.
- To get a copy of their personal data.
- To have their personal data corrected if inaccurate.
- To have their personal data deleted
- To prevent their personal data from being used for certain purposes: for example, one might want to have the data blocked for research purposes where it is held for other purposes.
- Under employment rights, not to be forced to disclose information to a prospective employer. No one can force another person to make an access request, or reveal the results of an access request, as a condition of recruitment, employment, or provision of a service. Where vetting for employment purposes is necessary, this can be facilitated where the individual gives consent to the data controller to release personal data to a third party.
- It should be noted that under the Freedom of Information Act 2014, records containing personal information may be released to a third party, where the public interest so requires.

In accordance with data subject rights under the General Data Protection Regulation (hereafter referred to as the 'GDPR'), and other associated legislation, St. Michael's House may receive a number of requests from data subjects. This policy provides details of what the data subject is entitled to and what employees should do to comply with their statutory obligations.

58. Subject Access Requests

59. Information the Data Subject is entitled to in response to a Subject Access Request

The data subject is entitled to receive confirmation within one month of the receipt of the request as to whether personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information **:-**

a. The purposes of the processing.

b. The categories of personal data concerned.

c. The recipients or categories of recipient to whom the personal data have been or will be disclosed, recipients in third countries or international organisations.

d. Where possible, the retention period for the personal data.

e. The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.

f. The right to lodge a complaint with the Data Protection Commission Ireland (DPC).

g. Where the personal data are not collected from the data subject, any available information as to their source.

h. The existence of automated decision-making (if applicable), including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

60. Key Steps for dealing with Subject Access Requests

- The GDPR does not set out any method for making a valid subject access request. Requests can be made by a data subject in writing or verbally through any medium e.g. a letter, via email, via social media platforms.

- The FOI and Data Protection Admin office, will deal with all Subject Access Requests. All requests should be referred to FOI and Data Protection Admin office or in their absence to St. Michael's House Data Protection Officer immediately

- St. Michael's House encourages data subjects making a Data Subject Access request to do so via the St Michael's House subject access request form which is available to download here:
  https://www.smh.ie/assets/files/pdf/data_protection_-_subject_access_request_form.pdf

- When a Subject Access Request is received by St. Michael's House (see sample letter of request in Appendix II), the employee/s who receive/s the correspondence will refer it directly to the FOI and Data Protection Admin office.

- The FOI and Data Protection Admin office will then notify St. Michael's House's relevant Department or section.

- The date of the request should be logged by the FOI and Data Protection Admin office as the relevant Data Protection legislation requires a response to a request to be issued within one month.

- If the FOI and Data Protection Admin office has reasonable doubts as to the identity of the requestor or reasonably requires additional information to locate any relevant data, the FOI and Data Protection Admin office may request additional information and / or evidence of identity from the requester such as a copy of a passport or driver's license. A response requesting proof of identification may be issued without undue delay. Where such a request is made, time will stop running for the purposes of the one-month period and will begin again when the request is complied with.

- No fee will be payable for data subject requests. However, where requests from a Data Subject are considered 'manifestly unfounded or excessive' St. Michael's House may charge a reasonable fee, considering, the administrative costs of providing the information requested.

- Searches will be conducted by relevant individuals in the relevant department/s and systems of St. Michael's House for the requested data both electronically and manually. The FOI and Data Protection Admin office will request the relevant individuals to provide an accurate estimate of the volume of data held and an estimate of the time that it would take to carry out a thorough review of the documentation.

- If the Subject Access Request is complex or where there are a number of such requests the period of one month may be extended by two months by St. Michael's House. In these circumstances St. Michael's House will inform the data subject, in writing, of such extension within one month of receipt of the request, together with the reasons for the delay (see sample letter in App III).

- If searches reveal a volume of personal data that is incapable of being provided within one month (or three months were the data subject has been notified), a response will be issued to the data subject by the FOI and Data Protection Admin office requesting further detail on the information they require and asking the subject to narrow the request where possible.

- If the data subject does not narrow the request and the FOI and Data Protection Admin office is satisfied that it will not be possible to comply with

the request within one month (or three months), he/she must respond to the subject providing a breakdown of the reasons why it will not be possible to provide the information within the prescribed period (see sample letter in Ap IV).

- Where a data subject has requested a copy of their data this should generally be provided, where possible, via the same format it was requested, unless the data subject has requested it be provided in another format. Staff should be conscious of the quality of records and ensure that photocopies are legible. Particular attention should be paid to handwritten text on records, which are to be photocopied. Material, considered not suitable for release under the regulation, should be redacted.

61. Exemptions

A number of exemptions exist that may apply to personal data held by St. Michael's House. Exempted information need not be provided to the data subject. This information may be redacted or if the entire document is exempt, it should not be provided. The Data Protection Admin should record all instances where an exemption is deemed to apply.

Opinion given in confidence about the requester: This threshold is very high and only applies if the opinion would not have been given but for an understanding that it would be treated in confidence and applies only in cases where confidentiality is of the utmost concern. (e.g., reports or references given by managers will not generally be protected as it is an expected part of their role to give opinions on staff which they are expected to stand over).

- Disproportionate effort: St. Michael's House is required to supply a requester with a copy of their own personal data in permanent form unless the supply of such a copy is not possible or would involve disproportionate effort. The DPC Ireland has indicated that this can only be relied on where producing the relevant personal data would be disproportionate to the benefit to be derived by the requester in receiving a copy of the data.

- Third Party Data: If St. Michael's House cannot comply with a request without releasing information relating to another individual then that information may be withheld unless such third-party consents. However, if it is possible to redact the information relating to the third party this should be done and the remaining information released. If St. Michael's House does not have the consent of the third party and it would be impossible to provide redacted documentation without revealing the identity of the third party, St. Michael's House can provide the data subject with a summary of the information held about him/her that does not reveal the identity of the third party.

- Repeated Access Requests: If St. Michael's House has previously provided the same information under an earlier access request it does not have to comply with an identical or similar request unless 'a reasonable interval' has elapsed.

In considering this the relevant data protection legislation requires consideration of the nature of the data, the purpose for which the data is processed and the frequency with which the data may be altered.

- Investigation/Prevention of an Offence: The mere existence of a criminal investigation does not permit the exercising of a blanket ban on all personal data nor is such a ban permanent and may no longer be applicable once an investigation has concluded and proceedings are no longer in danger of being compromised.

- Legal Professional Privilege: The Acts provide that the right of access does not apply to personal data in respect of which a claim of privilege could be maintained in proceedings in a court in relation to communications between a client and his professional legal advisers or between these advisers. In the view of the DPC this does not mean that the existence of legal proceedings between St. Michael's House and a requester precludes an access request under the Acts nor is it a justification for refusing a request. The DPC also considers that it does not exclude communications between St. Michael's House's legal advisers and a third party or that third party's legal advisers.

  Health & Social Work Data: The Data Protection Regulation SI No 82 of 1989 and SI No 83 of 1989 provide that health and social work data relating to an individual should not be made available to that individual in response to a Subject Access Request (SAR) if it would be likely to cause serious harm to the physical or mental health of the requester. St Michael's House has decision makers who will support the process of establishing whether serious harm may be caused. Any medical terms not understood should not be disclosed without first consulting medical personnel or some other suitably qualified health professional.

- The protection of public or national security or the protection of the rights and freedoms of other persons: St. Michael's House may withhold data if it is satisfied that this is a necessary and proportionate measure for the purposes of the protection of public or national security or the protection of the rights and freedoms of others.

62. Request for Rectification of Personal Data held by St. Michael's House

Data subjects have a right under Article 16 of the GDPR to the rectification of any inaccurate or incomplete personal data which is held by St. Michael's House.

This includes **:-**

- A right to have incomplete personal data completed.
- A right to have inaccurate personal data corrected.

If a requester informs St. Michael's House that their personal information is incorrect or incomplete, the Data Protection Admin must ensure that the

requester's corrected information is obtained and placed on file and inform the requester this has been done.
If St. Michael's House's records relating to an individual are incomplete the relevant St. Michael's House's business area must search for the missing information or obtain the complete information from the Data Subject. If a complaint or request for review is received by St. Michael's House, the rectification of inaccurate or incomplete personal data must be completed within one month of receipt of the request.

63. Request for Erasure of Personal Data held by St. Michael's House right to be forgotten

Under Article 17 of the GDPR, Data Subjects have a right to the erasure of any personal data which is held by St. Michael's House where one of the following conditions applies **:-**

1. The personal data are no longer necessary in relation to the purposes for which they were collected.

2. The data subject withdraws consent (this applies only where St. Michael's House is relying on consent only as a lawful basis to process the data).

3. The data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for direct marketing purposes.

4. The personal data has been unlawfully processed.

5. The personal data must be erased for compliance with a legal obligation to which St. Michael's House is subject.

Where a request is made for the erasure of personal data held by St. Michael's House and one of the above conditions applies, the request must be complied with within one month of receipt of the request.
The FOI and Data Protection Admin Office should be informed so that a record can be kept of the request.

64. What happens if a requester makes a complaint to the Data Protection Commission ?

If St. Michael's House fails to comply with a valid data access request, the data subject has the right to make a complaint to the Data Protection Commission.

Complaints should be made in writing, including email, to the Data Protection Commission at:
Data Protection Commission,
21 Fitzwilliam Square South Dublin 2 D02 RD28 Ireland
+353 578 684 800
Email: info@dataprotection.ie

The DPC will consider the matter and may investigate. If the DPC cannot arrange an amicable solution within a reasonable time, a formal decision will be made on whether to proceed with an investigation.
If the DPC finds St. Michael's House to be in breach of data protection legislation following an inquiry or investigation, it may order corrective action to be taken. Failure to comply with a corrective action constitutes a further breach of legislation. For further information contact the FOI and Data Protection Admin Office or consult www.dataprotection.ie.

65. Roles / Responsibilities of the Chief Executive Officer

The Chief Executive Officer has overall responsibility for ensuring compliance with Data Protection legislation. However, all employees of St. Michael's House who collect and / or control the contents and use of personal data are also responsible for compliance with Data Protection legislation. St. Michael's House will provide support, assistance, advice and training to all relevant departments, and staff to ensure it is able to comply with the legislation. The Chief Executive Officer will appoint the redacting officers and designate the reviewing officers.

Contact Person:
FOI and Data Protection Admin Office
St Michael's House
Ballymun
info@smh.ie
(01)8840200

66. Procedures and Guidelines

This policy supports the provision of a structure to assist in St. Michael's House's compliance with Data Protection legislation, including the provision of best practice guidelines and procedures in relation to all aspects of Data Protection.

67 Review

This Policy will be reviewed regularly considering any legislative or other relevant developments including guidance from the DPC. It shall be the responsibility of the Data Protection Officer to keep this policy updated.

68. Definitions from GDPR and Associated Legislation

The following definitions are taken from the General Data Protection Regulation and associated legislation. Full copies of the legislation are available at the Data Protection Commissioner's website www.dataprotection.ie.

1. 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

2. 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

69. Sample Letters Requesting More Information Subject Access Requests

Please see below, sample wording for letter to access data held under the General Data Protection Regulations. When requesting information, it is important to give any details that will help the person to identify you and find your data – for example a staff number, any previous address, or your date of birth; and be clear about which details you are looking for if you only want certain information. This will help simplify the search and respond more efficiently. No fee will apply to any application for information under the Data Protection Act.

FOI and Data Protection Admin
Ballymun Road
Dublin D09DX37

1. Request for rectification of personal data held by St. Michael's House

   Please change (e.g., my address on your system or other personal data) as the information you hold on me is incorrect.

   Or

   Under the General Data Protection Regulation and associated legislation and Article 16 of the General Data Protection Regulation, I wish to make a request for the rectification of inaccurate/incomplete personal information you keep about me, on computer or in manual form.

   [Insert relevant information to assist St. Michael's House to identify you and find your data. Provide full details of the inaccurate or incomplete nature of the data and provide the correct information that you wish St. Michael's House to update and rectify].

2. Request for erasure of personal data held by St. Michael's House (right to be forgotten)

   The information (specify what) you hold on me, is no longer required by you (or any of the other reasons set out in the policy) please delete it immediately.

   Or

   Under the General Data Protection Regulation and Article 17 of the EU General Data Protection Regulation, I wish to make a request for the erasure of personal information you keep about me, on computer or in manual form.

   [Insert relevant information to assist St. Michael's House to identify you and find your data. Provide full details of the data you seek to have erased. It is important to clarify whether you wish for some or all your information to be erased].

Yours sincerely,

[Name] Email Address Phone Number

70. Sample letter Not Possible to Provide the Information within the Time Frame

Dear [Mr./Ms. Data Subject],

We refer to your Subject Access Request of [insert date of request] received by us on [insert date received by St. Michael's House].
[INSERT REASONS FOR DELAY]
For these reasons it will be impossible to provide you with the relevant documentation within the one-month statutory timeframe. Having regard to [insert relevant provision of the Act], we now require a further period of [insert time period- no longer than 3 months from receipt of request] to [respond to your request/to consider your request].

Yours faithfully,

[Name]
[Insert]

71. Sample Letter Requesting Reduction of Scope of Subject Access Request

Dear [Mr./Ms. Data Subject],

We refer to your Subject Access Request of [insert date of request] received by us on [insert date received by St. Michael's House].
We hold personal data in relation to you from [insert date of first personal data obtained] until [the present time/ date of most recent personal data held].
We have carried out a review of our system and files and confirm that we have approximately [insert figure] soft copy documents which may be of relevance. In addition, we have approximately [insert number] of hard copy documents which may contain information relevant to your request.
The processing of this amount of data for the purpose of supplying you with a copy would be impossible within the one month [or three months] statutory timeframe and having regard to [insert relevant provision of the Act], we now require you to limit the scope of your request to a specific time and/or to specify the subject matter of the documentation required by you.

We await hearing from you.

Yours faithfully,

[Name]
[Insert]

72. Schedule of documents Released

Dear [Mr./Ms. Data Subject],

We refer to your Subject Access Request of [insert date of request] received by us on [insert date received by St. Michael's House].

In compliance with your request made pursuant to Section [x] and Article 16 of the General Data Protection Regulation we now enclose the following documents for your attention.

[SCHEDULE OF DOCUMENTS]

We trust this is in order.

Yours faithfully

73. SUBJECT ACCESS REQUEST FORM

For Records Under the General Data Protection Regulation (GDPR)

Under the General Data Protection Regulation (GDPR) it is your right to request a copy of any personal data that we hold on you. Please note that this form is to support you with the Subject Access Request process, however we will accept your request if made in another format. If you want to submit a request, send the completed form or letter to the office of the Data Protection Admin Office in St. Michael's House, Ballymun Road, Dublin 9.

Details of Applicant

Please use BLOCK letters:

Applicant's Name: _____ **Relationship** _____

Employee / Service User's Name: _____

Where employed / What services used : _____ **Date of Birth:** _____

Postal Address:

Email Address:

Telephone Numbers:

Information / File Contents Requested:

Please state the Specific information you are requesting :-.

Please supply all home address of the Subject Access Request

Personal Information: *Before you are given access to personal information relating to yourself, you may be required to provide proof of your identity. Parents and Guardians submitting Subject Access Requests must state clearly why they are requesting the records.*

Form of Access: My preferred form of access (please tick as appropriate)
To receive copies of the records by post
To receive copies of the records by email

Signed_____
_____**Date**_____

_____

Office Use Only: Date Subject Access Request Received:_____

Identity Verified **Consent Confirmed**:

74

APPENDIX THREE

Data Breach Management.

St. Michael's House

Data Breach Management Policy

74.	Appendix 111 DATA BREACH MANAGEMENT POLICY INDEX
75	Summary of St Michael's House's Data Breach Policy
76	Data protection Officer Contact Details
77	Basic Security considerations
78	What is a personal Data Breach ?
79	Definitions
80	Types of personal Data Breaches
81	Data Breach Notification Procedures for all St Michaels House Employees and Contractors
82	When we notify the Data protection Commission Ireland
83	Processor obligations
84	Information to be provided to the data Commission Ireland
85	Notification in phases
86	Breaches affecting individuals in more than one Member State
87	Conditions where notification is not required
88	Stop
89	Internal Investigation
90	Communication to the data subject
91	Informing individuals
92	Information to be provided
93	Contacting Individuals
94	Conditions where notification is not required
95	Accountability and Record keeping
96	St. Michaels House's Data Breach Log
97	Data Breach : Notice to Supervisory Authority
98	Data Breach : Notice to Data Subjects
99	Data Breach : Incident Report Form Sample
100	BLANK INCIDENT REPORT FORM
101	Change History Record

74. ST MICHAELS HOUSE DATA BREACH MANAGEMENT POLICY

St. Michael's House is obliged in certain circumstances under the General Data Protection Regulation (the "GDPR") to report a personal data breach ("breach") to the national supervisory authority (Data Protection Commission (''DPC'') Ireland) within 72 hours of becoming aware of the incident and, in certain cases, communicate the breach to the individuals whose personal data has been affected by the breach.

In most cases in which St. Michael's House handles personal data, it acts as the "Data Controller." However, there may be instances where St. Michael's House is the "Data Processor." Under the GDPR, Data Controllers report to the DPC Ireland and Data Processors have obligations to report the occurrence of a personal data breach to the Data Controller.

When making a notification to the Data Protection Commission (DPC) Ireland, St. Michael's House can obtain advice on whether the affected individuals ("data subjects") need to be informed. The DPC Ireland may order St. Michael's House to inform those individuals about the breach. Communicating a breach to individuals allows St. Michael's House to provide information on the risks presented because of the breach and the steps those individuals can take to protect themselves from its potential consequences. The focus of any breach response plan should be on protecting individuals and their personal data. Consequently, breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data. At the same time, it should be noted that failure to report a breach to either an individual or a supervisory authority may mean that under Article 83 of the GDPR a possible sanction can be imposed on St. Michael's House by the Data Protection Commission.

75 Summary of St. Michael's House's Data Breach Policy:

1. Information concerning all data security-related events should be immediately directed to the Data Protection Officer and the person with responsibility for the area in which the potential breach occurred, establishing the existence and facts of breach, and assessing the related risks.

2. The risk of individuals having their privacy impacted because of a breach should then be assessed (likelihood of no risk, risk, or high risk).

3. Notification to the DPC Ireland and potentially communication of the breach to the affected individuals should be made, if required.

4. At the same time, St. Michael's House should take all necessary steps to contain and recover the personal data that has been disclosed, lost, or stolen.

76. Data Protection Officer Contact Details :

XpertDPO
20 Harcourt Street,
Dublin 2

77. Basic Security Considerations

By using appropriate technical and organisational measures, personal data shall be processed by St Michael's House employees in a manner that ensures the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. St.

further information see St Michaels House's new Information Security Policy .

a) The "destruction" of personal data is where the data no longer exists, or no longer exists in a form that is of any use to the controller.

b) "Damage" should also be relatively clear: this is where personal data has been altered, corrupted, or is no longer complete.

c) The "loss" of personal data should be interpreted as the data may still exist, but the controller has lost control of it or access to it or no longer has it in its possession.

d) Unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR

78. What is a personal Data Breach ?

A personal data breach is a type of security incident. The consequence of such a breach is that the controller will be unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 of the GDPR.
All data breaches must be reported by St. Michael's House staff members to the Data Protection Officer immediately regardless of whether it is a confirmed personal data breach or not. The Data Protection Officer shall conduct his/her own assessment of whether the breach constitutes a personal data breach. If the Data Protection Officer is not present, all staff are required to report the incident to the FOI and Data Protection admin Office.

79. Definition

The GDPR defines a "personal data breach" in Article 4(12) as: *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed".*

80. Types of personal data breaches

Personal data breaches can be categorised according to the following three well-known information security principles:

- **"Confidentiality breach"** - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- "**Availability breach**" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.
- "**Integrity breach**" - where there is an unauthorised or accidental alteration of personal data.

A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage.

This can include:

- loss of control over their personal data
- limitation of their rights
- discrimination
- identity theft or fraud
- financial loss
- unauthorised reversal of pseudonymisation
- damage to reputation,
- loss of confidentiality of personal data protected by professional secrecy
- any other significant economic or social disadvantage to those individuals.

In the event of a confirmed personal data breach, St. Michael's House is required to notify the DPC Ireland unless it is unlikely to result in a risk of such adverse effects taking place. Where there is a likely high risk of these adverse effects occurring, St. Michael's House is required to communicate the breach to the affected individuals as soon as is reasonably feasible.

81. Data Breach Notification Procedure for all St. Michael's House Employees and Contractors

All employees and contractors (including third party contractors) of St. Michael's House are required to notify data breaches to the Data Protection Officer immediately. A copy should be sent to the Head of Communications , St Michael's House.

The person who discovers the incident must document the incident with as much detail as possible; however, the process of documentation must not delay eradication of the incident.
A detailed account of the breach should be recorded accurately on the St Michaels House Incident Report Form Ap111 (at end). This will include the following areas :-
-the date and time the breach occurred
-who reported the breach
-description of the breach
-details of any ICT systems involved
-description of the nature of the data stored on the ICT system

Where an employee is not sure whether an incident or event constitutes a data breach, they should report it to the Data protection Officer to make that determination.
Data breaches involve a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored, or otherwise processed.

Practical examples of data breaches include but are not limited to the following:

- sending an email containing personal data to the wrong recipient
- unauthorised publication of personal data to a public forum
- loss or theft of a St. Michael's House issued electronic device
- loss or theft of a hard copy file containing personal data

- an IT security incident - i.e., hacking, phishing, or ransomware
- unauthorised or accidental disclosure of personal data to a third party
- unauthorised physical access to the building by a third party.

Failure to report a data breach or a potential data breach immediately may result in disciplinary action.

Employees must assist the Data Protection Officer in any internal investigations or investigations by the DPC Ireland.

Employees shall not disclose details of any data breach or security incident to the media without the prior approval of the Head of Communications St. Michael's House.

Failure to adhere to this procedure, whether it be by delay or failure to report the breach to St. Michael's House may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment.

82. When to notify the Data Protection Commission Ireland

In the case of an actual or confirmed personal data breach, St. Michael's House shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the DPC Ireland, unless the personal data breach is **unlikely** to result in a risk to the rights and freedoms of natural persons.

Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by a reasoned justification for the delay.

Any delay in reporting allows the incident to escalate or for further consequential incidents to occur. Without timely visibility of the incident through reporting St. Michael's House may not be able to fulfil its legal obligations

See sample notification letter at **App 1.**

83. Processor Obligations

In most cases in which St. Michael's House handles personal data, it acts as the "Data Controller". However, there may be instances where St. Michael's House is the "Data Processor". Under the GDPR, Data Controllers and Processors have obligations to report the occurrence of a personal data breach.
The controller retains overall responsibility for the protection of personal data, but the processor has an important role to play to enable the controller to comply with its obligations; and this includes breach notification.

All processing by a processor shall be governed by a contract (and an associated Data Processing Agreement) or other legal act. The contract or legal act shall stipulate that the processor "assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor".

If a processor is used by a controller and the processor becomes aware of a breach of the personal data it is processing on behalf of the controller, it must notify the controller in writing and "without undue delay".

The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as "aware" once the processor has become aware. The obligation on the processor to notify its controller allows the controller to address the breach and to determine whether it is required to notify the supervisory authority.

84. Information to be provided to the Data Protection Commission Ireland

Where the Data Protection Officer notifies a breach to the supervisory authority, at the minimum, they should :-

a) Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.

b) Communicate the name and contact details of St. Michael's House Data Protection Officer or other contact point where more information can be obtained.

c) describe the likely consequences of the personal data breach.

d) describe the measures taken or proposed to be taken by St. Michael's House to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

e) If a processor is the root cause of a breach, the name and role of the processor should also be communicated to the DPC Ireland.

64 Notification in phases

Depending on the nature of a breach, further investigation may be necessary to establish all the relevant facts relating to the incident. St. Michael's House will not always have all the necessary information concerning a breach **within 72 hours** of becoming aware of it, as full and comprehensive details of the incident may not always be available during this initial period. Therefore, where it is not possible to provide all information regarding the breach to the DPC Ireland at the same time, the information may be provided in phases without undue further delay.

It is more likely this will be the case for more complex breaches, such as some cyber security incidents where, for example, an in-depth forensic investigation may be necessary to fully establish the nature of the breach and the extent to which personal data have been compromised. Consequently, in many cases St. Michael's House will have to conduct further investigations and follow-up with

additional information at a later point. St. Michael's House can be assisted by FOI & Data protection Admin Office in investigations.

Where notification in phases is deemed necessary by the Data Protection Officer, he/she must give reasons for the delay. Therefore, when the Data Protection Officer first notifies the supervisory authority, he/she should also inform the supervisory authority if he/she will provide more information later. The supervisory authority should agree how and when additional information should be provided.

86. Breaches affecting individuals in more than one Member State

Where St. Michael's House engages in the cross-border processing of personal data, a breach may affect data subjects in more than one Member State. Where this occurs and notification is required, the controller will need to notify the lead supervisory authority. As Ireland is the place of main establishment within the European Union, the DPC Ireland is the lead supervisory authority for St. Michael's House unless this is objected to in which case a decision will be taken by the European Data Protection Board.

87 Conditions where notification is not required

Breaches that are "unlikely to result in a risk to the rights and freedoms of natural persons" do not require notification to the supervisory authority. An example might be where personal data are already publicly available and a disclosure of such data does not constitute a likely risk to the individual.

An example provided by the Article 29 Working Party is as follows:

A breach that would not require notification to the supervisory authority would be the loss of a securely encrypted mobile device, utilised by the controller and its staff. Provided the encryption key remains within the secure possession of the controller and this is not the sole copy of the personal data then the personal data would be inaccessible to an attacker. This means the breach is unlikely to result in a risk to the rights and freedoms of the data subjects in question. If it later becomes evident that **the encryption key was compromised** or that the encryption software or algorithm is vulnerable, then the risk to the rights and freedoms of natural persons will change and thus notification may now be required.'

88. Stop

The Data Protection Officer will stop the notification process if it is determined that there is no incident to be managed and will update the person who reported the incident, through the FOI & Data Protection Admin Office informing them and clarifying why the situation is not classified as an incident and why further action is not required.

89. Internal Investigation

The Data Protection Officer is also required to info the HSE Consumer Affairs Officer of the relevant HSE region where the data breach has occurred. This will

be a detailed written report of the data breach like that required by the DPC Ireland. The Data Protection Officer, in consultation with the Chief Executive Officer (CEO) will lead an investigation regarding all issues surrounding the data breach. The nature of such an investigation will vary from case to case, depending on the circumstances and seriousness of the data breach. The primary issue for consideration will be the question of informing those individual directly affected by the loss and how it might be done. The Data Protection Officer will also take into consideration the recommendations from the Data Protection Commission and the Consumer Affairs Officer of the HSE.
Following the investigation, a thorough review of the incident will occur to ensure that steps taken during the management of the Data Breach were appropriate, areas of improvement for data processing and security are identified and used for shared learning across St Michael's House to enhance the transparency, accountability, safety, and privacy of personal and sensitive information.

90. Communication to the data subject

91. Informing individuals

In certain cases, as well as notifying the DPC Ireland, the Data Protection Officer is also required to communicate a breach to the affected individuals when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. If notification to the affected individuals is required, St. Michael's House shall communicate the personal data breach to the data subject without undue delay. A template for informing Data Subjects of Data Breaches is provided in **App II** below**.**

When notifying individuals, St. Michael's House should seek to provide specific information about steps individuals should take to protect themselves. Depending on the nature of the breach and the risk posed, timely communication will help individuals to take steps to protect themselves from any negative consequences of the breach.

92. Information to be provided

When notifying the affected individuals, St. Michael's House should at a minimum provide the following information:

- A description of the nature of the breach
  The name and contact details of St. Michael's House's or other contact point
- A description of the likely consequences of the breach; and
- A description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

93. Contacting Individuals

The relevant breach should be notified to the affected individuals directly, unless doing so would involve a disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

94. Conditions where notification is not required

If a breach occurs and any of the below conditions apply, notification to the affected individuals is not required:

- If St. Michael's House has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it. This could, for example, include protecting personal data with state-of-the-art encryption.

- If immediately following a breach, St. Michael's House has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise. For example, depending on the circumstances of the case, St. Michael's House may have immediately identified and acted against the individual who has accessed personal data before they were able to do anything with it. Due regard still needs to be given to the possible consequences of any breach of confidentiality, again, depending on the nature of the data concerned.

- If it would involve disproportionate effort to contact individuals, perhaps where their contact details have been lost because of the breach or are not known in the first place. For example, where St. Michael's House's property is flooded and destroys documents containing personal data which were stored only in paper form. In those circumstances it may not be possible to contact the individuals. Instead, St. Michael's House must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner.

  If St. Michael's House's Data Protection Officer seeks to rely on one of these conditions to avoid the requirement to notify individuals of a personal data breach, the reasoning behind the decision should be recorded on St. Michael's House's Data Breach Log (see next section) and details of such reasoning provided to the DPC Ireland. If the DPC Ireland determines that the decision not to notify data subjects is not well founded, it may consider employing its available powers and sanctions.

95 Accountability and Record Keeping

96. St. Michael's House's Data Breach Log

The Data Protection Officer must maintain a Data Breach Log which records:

- The occurrence of a data breach
- The cause of the breach
- The personal data affected
- The reasoning behind a decision to notify or not to notify
- The reasons why the Data Protection Officer considers the breach is likely / unlikely to result in a risk to the rights and freedoms of individuals
- Reasons for any delay in reporting
- A list of individuals affected
- The effects of the breach

- Remedial steps taken in response.

It is essential that the Data Breach Log is maintained as the documentation shall enable the DPC Ireland to verify St. Michael's House's compliance with the GDPR. Regardless of whether a breach needs to be notified to the supervisory authority, it should be recorded in the log.

Failure to properly document a breach can lead to the supervisory authority exercising its powers and imposing an administrative fine.

97. SAMPLE LETTERS DATA BREACH: NOTICE TO SUPERVISORY AUTHORITY

Dear Sirs,

We are the data controller in relation to [ ].
We are writing in accordance with our obligations under Article 33 of the GDPR.
It has come to our attention that on [date] [describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned].

The Data Protection Officer of St. Michael's House and their contact details are as follows:
Data Protection Officer
XpertDPO
20 Harcourt Street,
Dublin 2

We are reporting this incident because currently having regard to the information available to us, we believe that [describe the likely consequences of the personal data breach].
St. Michael's House has taken the following measures to address the personal data breach and mitigate its possible adverse effects:
(a)
(b)
(c)
(d)

[In the event that a data processor who has a contract with St. Michael's House is the root cause of the breach, you should identify the processor at this point to include their name and role of the processor]

Yours faithfully,
XXX
[Insert].

98. DATA BREACH: NOTICE TO DATA SUBJECTS

[On headed notepaper of St. Michael's House]
[ADDRESSEE]
[ADDRESS LINE 1]
[ADDRESS LINE 2]
[POSTCODE]

[DATE]

Notification of a personal data security breach

Dear [DATA SUBJECT],

We are sorry to inform you of a breach of security that has resulted in the [loss OR unauthorised disclosure OR destruction OR corruption] of your personal data. The breach was discovered on [DATE] and is likely to have taken place on [DATE]. As a result of our investigation of the breach, we have concluded that: THE Following PERSONAL DATA PLACED AT RISK

The breach affects the following types of information:

- [TYPES OF INFORMATION, FOR EXAMPLE, FINANCIAL OR SENSITIVE PERSONAL DATA AND DETAILS OF THE EXTENT].

It is likely that the breach affects around [NUMBER] data subjects.

- The information has been [accidentally or unlawfully destroyed OR lost OR altered OR disclosed without authorisation OR accessed by [[NAME OR DESCRIPTION OF ORGANISATION] OR an unauthorised person]].
- The breach occurred under the following circumstances and for the following reasons:
  - [CIRCUMSTANCES].
  - [REASONS].

The breach may have the following consequences and adverse effects on the affected data subjects:

- [CONSEQUENCES].
- [ADVERSE EFFECTS].

We have [received [NUMBER] of complaints OR not received any complaints] from the affected individuals.

We have taken the following steps to mitigate any adverse effects of the breach: CONTAINMENT AND RECOVERY

We [have taken OR propose to take] the following measures to address the breach and to minimise and mitigate its effects on the affected individuals:

- [MEASURES].

The information has [not] been recovered [and the details are as follows:

- [DETAILS OF HOW AND WHEN IT WAS RECOVERED].]

We have also taken the following steps to prevent future occurrences of the breach:

- [REMEDIAL ACTION TAKEN].

[The facts surrounding the breach, the effects of that breach and the remedial action taken have been recorded in a data breach inventory maintained by the [data controller OR the company].]

We recommend that you take the following measures to mitigate possible adverse effects of the breach:

- [MEASURES].

[We informed the Office of the Data Protection Commissioner Ireland of the breach on [DATE]].

You can obtain more information about the breach from any of the following contact points:

Data Protection Officer
XpertDPO
20 Harcourt Street,
Dublin 2

The above mentioned is the Data Protection Officer of St. Michael's House and he/she may be contacted directly or via Data Protection Office Administration, St Michael's House, info@smh.ie
(01)8840200

We apologise for any inconvenience this breach may cause you.
Yours sincerely,
XXX
[Insert].

99. Data Breach : Incident Report Form

Sample data Breach Report Form

St. Michael's House Data Protection Breach Incident Report Form

INCIDENT DETAILS	
Service / Department Name:	**Willowriver**
Detailed description of the Incident: **(Internal incident/external incident)**	**Document with service users name and medication requirements blew out of the recycling bin on to the street when the bin had been left out for collection**
Date and Time Incident Occurred:	**15/02/2023 @11.25h**
Name of Individual Reporting the Incident:	**Joe Blogs**
Incident Reported to Line Manager and Data Protection Officer:	**15/02/2023**
Type of Personal Data Involved. Any Data of a Sensitive Nature:	**Information regarding the service user's medication requirements**
No. of Individuals Affected by the Breach:	**1**
Cause of the Incident:	**Information was placed in the recycling bin for disposal.**
Were Affected Individuals Contacted?	**Yes**
Was the Data Encrypted or Anonymised?	**No**
Details of any IT Systems Involved in The Breach	**N/A**
Safety Control Measures Enacted	**All information containing service users' information to be shredded and to confidentially dispose of potentially sensitive documentation**

Signature: _____ **Date:** _____

Received by DPO _____ **Date:** _____

100. Blank Breach Report Form

St. Michael's House Data Protection Breach Incident Report Form	
INCIDENT DETAILS	
Service / Department Name:	
Detailed description of the Incident: **(Internal incident/external incident)**	
Date and Time Incident Occurred:	
Name of Individual Reporting the Incident:	
Incident Reported to Line Manager and Data Protection Officer:	
Type of Personal Data Involved. Any Data of a Sensitive Nature:	
No. of Individuals Affected by the Breach:	
Cause of the Incident:	
Were Affected Individuals Contacted?	
Was the Data Encrypted or Anonymised?	
Details of any IT Systems Involved in The Breach	
Safety Control Measures Enacted	

Signature: _____ **Date:** _____

Received by DPO _____ **Date:** _____

101. Change History Record

Data Protection Policy incorporating :-
Policy for Retention of Records (Appendix 1)
Subject Access Request Policy (Appendix 2)
Data Breach Management Policy (Appendix 3)

Issue	*Description of Change .*	*Approval*	*Date*
	Index change includes new appendix 1,2 and 3 now part of this policy		
	Ist paragraph Chief Executive Officer entered		
	2.1 Board of Directors inserted		
	2.5 Data Protection Officer inserted		
	2.6 Director of Human Resources inserted		
	3 Child First Act 2015 inserted		
	3.1 b) To comply with all legal requirements inserted		
	3.1 c) locked and secured in all locations		
	3.1 c) Digital records are stored on servers which can only be accessed by password protected computers and laptops with adequate encryption and firewall software.		
	3.1 d) to prevent loss of personal data to and from SMH…….		
	3.2 c) as per 3.1 b) and as per 3.1 c) for digital		
	3.2 d) to prevent loss of personal data to and from SMH…….		
	3.3 c) as per 3.1 b) and as per 3.1 c) for digital		
	3.3 d) to prevent loss of personal data to and from SMH…….		
	3.4 c) as per 3.1 b) and as per 3.1 c) for digital .		
	3.4 d) to prevent loss of personal data to and from SMH…….		
	4. The Chief Executive Officer inserted		
	5.2.1 The Chief Executive Officer inserted		
	5.2.2 by the Director of Human Resources		
	5.3 The Director of Human Resources		
	5.3.1 The Director of Human Resources		
	5.2.3 the Data Protection Officer will ensure on an annual basis, that all data collection methods are reviewed.		
	5.3.2 The Data Protection Officer inserted		
	5.3.3 in writing or by email inserted		
	5.4.3 The Chief Executive Officer inserted x 2		
	5.5 The Director of Human Resources inserted x 4		
	6.2.1 Subject Access Request Policy (Appendix 11 to this policy)		
	6.2.2 as per 6.2.1		
	7.5 using standard consent documents from parent or guardians		
	8.2 updated to include contracts and Contractors		
	9.1 in line with the Data Breach Management Policy (Appendix 3 to this policy)		
	9.1 The Data Protection Officer		
	9.2 The Data Protection Officer		
	10.2 The Data Protection Officer		
	14.4 The Data Protection Officer		

	14.5 The Data Protection Officer		
	14.6 The Data Protection Officer		
	14.6 The Board of Directors		
	15. The Chief Executive Officer		
Appendix 1	**Policy for the Retention of Records**		
Appendix 1	**19 New Contents Page**		
Appendix 1	**21 Chief Executive Officer**		
Appendix 1	**21 the HSE and St Michaels House Retention Schedule**		
Appendix 1	**29 in accordance with HSE and St Michaels House retention policy, list the records and then destroy the records.**		
Appendix 1	**32 the Chief Executive Officer to be satisfied that the methods used provide adequate**		
Appendix 1	**Paragraph 34 has now changed to the Retention Schedule.**		
Appendix 2	**35 Subject Access Request Policy New Content page**		
Appendix 2	**Index sheet amended former Appendix now AP 1 to V**		
Appendix 2	**39 FOI and Data Protection Admin office x 7**		
Appendix 2	**39 May** inserted		
Appendix 2	**40 The Data Protection Regulation SI No 82 of 1989 and SI No 83 of 1989 provide that health and social work data relating to**		
Appendix 2	**41 FOI and Data Protection Admin office**		
Appendix 2	**42 FOI and Data Protection Admin office**		
Appendix 2	**44 Chief Executive Officer**		
Appendix 2	**44 FOI and Data Protection Admin Office, St Michael's House Ballymun inf@smh.ie (01)8840200**		
Appendix 2	**46 Data Protection Officer**		
Appendix 2	**46 The Chief Executive Officer**		
Appendix 2	**48 FOI & Data Protection Admin**		
Appendix 2	**52 SUBJECT ACCESS REQUEST FORM**		
Appendix 3	**53 Data breach Management Policy**		
Appendix 3	**54 Data Breach Management Policy Index**		
Appendix 3	**54 Data Protection Officer**		
Appendix 3	**56 Information Security Policy**		
Appendix 3	**57 Data Protection Officer x 3 FOI & Data Protection Admin**		
Appendix 3	**60 Data Protection Officer x 2**		
Appendix 3	**60 Head of Communications X 2**		
Appendix 3	**60 a and b Data Protection Officer x 2**		
Appendix 3	**64 FOI & Data protection Admin Office**		
Appendix 3	**64 Data Protection Officer x 2**		
Appendix 3	**67 Data Protection Officer, FOI & Data protection Admin Office**		
Appendix 3	**68 Data Protection Officer**		
Appendix 3	**70 Data Protection Officer x 2**		
Appendix 3	**75 Data Protection Officer x 2**		
Appendix 3	**75 Chief Executive Officer**		
Appendix 3	**76 App1, 11, 111 Data Protection Officer x 3**		