DATA PROTECTION POLICY & PROCEDURE **GV24**

Next Review:	**Q4 - 2021**

DOCUMENT CONTROL			
Written or Revised	By	Version	Changes Committee Approval
February 2020	Sandra Britten & Melanie McLaughlin	1.0	Original Version.

RELATED HOSPICE DOCUMENTS & POLICIES	
C05	Disclosure/Provision of Information Policy & Procedure
C52	Records Management and Record Keeping Policy & Procedure.
NC14	Confidentiality Policy & Procedure
HR23	Disciplinary Policy & Procedure
HR08	Sickness Policy & Procedure
HR15	Equality & Diversity Policy & Procedure
HR38	Disclosure and Barring Service (DBS) and Employment Checks Policy.

REFERENCES
Information Governance Alliance (IGA)
Guide to Confidentiality 2013, NHS Digital Guidance
Caldicott Review 2013
Information Commissioners Office (ICO) Codes of Practice
Confidentiality: NHS Code of Practice, Department of Health 2003
Records Management Code of Practice for Health & Social Care 2016

LEGISLATION
General Data Protection Regulations (GDPR) 2018.
Data Protection Act 2018
Health and Social Care (Safety & Quality) Act 2015
Computer Misuse Act 1990
Human Rights Act 1998 (Article 8)
Common Law Duty of Confidentiality
Access to Health Records Act 1990
Crime and Disorder Act 1998
Mental Capacity Act 2005
Freedom of Information Act 2000
Privacy and Electronic Communications Regulations 2003
Regulation of Investigatory Powers Act 2000

1.0 INTRODUCTION

Data protection laws exist to strike a balance between the rights of individuals to privacy and the ability of organisations to use data for legitimate business purposes.

The General Data Protection Regulation and Data Protection Act 2018 came into force on 25 May 2018 and replace the Data Protection Act 1998 which came into force on 1 March 2000. The Regulation/DPA is concerned with "personal and sensitive data" about living, identifiable individuals which is "automatically processed or manually stored as part of a relevant filing system or accessible record". It need not be particularly sensitive information, indeed it can be as little as a name and address.

Alice House Hospice needs to keep certain information about its employees, volunteers, service users, donors, supporters, customers and other users to allow it to monitor performance, achievements, service users care, employment, donations, health and safety, for example.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Alice House Hospice must comply with the Data Protection Principles, which are set out in the General Data Protection Regulations (GDPR) 2018.

In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.

Alice House Hospice and all employees or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, Alice House Hospice has developed the Data Protection Policy and Procedure.

2.0 SCOPE

This policy covers all identifiable information created, processed and stored on living individuals, employees, volunteers, service users, donors, supporters, cutomers and other users. Throughout this document the term “service user” is used to refer to an individual who is receiving a service from the Hospice.

3.0 STATUS

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by Alice House Hospice. Any failures to follow the policy can therefore result in disciplinary proceedings. Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the Deputy Chief Executive/Director of Information Governanace.

4.0 DUTIES AND RESPONSIBILITIES

4.1 Employment/Volunteering

All staff and volunteers are responsible for:

- Checking that any information that they provide to Alice House Hospice in connection with their employment/volunteering is accurate and up to date.
- Informing Alice House Hospice of any changes to information, which they have provided, ie changes of address.
- Informing Alice House Hospice of any errors or changes in employee/volunteer information. Alice House Hospice cannot be held responsible for any such errors unless the employee has informed the Senior Manager Corporate Services.

4.2 Data Security

All staff and volunteers are responsible for ensuring that:

- Any personal data, which they hold, is kept securely, for example:
    - Kept in a locked filing cabinet; or
    - In a locked drawer.
- The computer is password protected.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual staff member.

4.3 Rights to Access Information

Staff, volunteers, service users, donors, supporters, cutomers and other users of Alice House Hospice have the right to access any personal data that is being kept about them either on computer or paper files. Any person who wishes to exercise this right should make the request in writing to the Deputy Chief Executive/Director of Information Governance.

Alice House Hospice aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days from the recorded request.

4.4 Subject Consent

In many cases, Alice House Hospice can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to Alice House Hospice processing some specified classes of personal data is a condition of employment for employees.

4.5 Processing Sensitive Information

Sometimes it is necessary to process sensitive information, for example racial or ethnic origin, religious or philosphical beliefs and health. This is to ensure that Alice House Hospice can safely deliver service users care services and operate Hospice policies, such as the Sickness Policy or Equal Opportunities Policy.

Alice House Hospice will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma, diabetes or disabilities.

4.5.1 Staff and Volunteers

Alice House Hospice will only use the information in the protection of the health and safety of the individual, but will need consent to process for example, in the event of a medical emergency. Offers of employment may be withdrawn if an individual refuses to consent to this, without good reason.

This processing is necessary for employement (GDPR Article 9 (1)(b)).

4.5.2 Service Users

Alice House Hospice will use this information to direct, manage and deliver the care you receive to ensure that:

- The doctors, nurses and other healthcare professionals involved in your care have accurate and up to date information to assess your health and decide on the most appropriate care for you.
- Healthcare professionals have the information they need to be able to assess and improve the quality and type of care you receive.
- Appropriate information is available if you see another doctor, or are referred to a specialist or another part of the NHS.

This processing is necessary to perform a public task (GDPR Article 6(1)(e))and necessary for the provision of health or social care treatment (GDPR Article 9(2)(h)).

4.6 Crimincal Offence Data

Information relating to criminal convictions and offences are not 'special categories' data, however the DPA does deal with this type of data in a similar way to special category data and sets out specific conditions providing lawful authority for processing it (Article 10 provisions as a basis for processing such data).

Criminal offence data Article 10 of the GDPR/DPA 18 stipulates that processing criminal offence data must be authorised by Member State Law, providing for appropriate safeguards for the rights and freedoms of data subjects.

4.6.1 Staff and Volunteers

Alice House Hospice will use this information for the following employment purposes:

GDPR Article 6(1)(e)) for the performance of a task carried out in the public interest or in the exercise of official authority….'
GDPR Article 9(2)(b) for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of employment.

4.6.2 Service Users

Alice House Hospice will use this information for the purposes of safeguarding children and vulnerable adults:

- GDPR Article 6(1) (e) for the performance of a task carried out in the public interest or in the exercise of official authority….'

- GDPR Article 9(2)(b) for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of … social protection law in so far as it is authorised by Union or Member State law…'

4.7 Retention of Data

Alice House Hospice will keep some forms of information for longer than others. Retention of data is documented within the Records Management and Record Keeping Policy & Procedure.

4.8 Conclusion

Compliance with GDPR is the responsibility of all employees of Alice House Hospice. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken.

5.0 GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018

5.1 Employee Guidelines

1. Employees have a duty to make sure that they comply with the data protection principles, which are set out in this policy. In particular, employees must ensure that records are:
   a. accurate;
   b. up-to-date;
   c. fair;
   d. stored and disposed of safely, and in accordance with Alice House Hospice policies.
2. Employees are responsible for ensuring that all data they are holding is kept securely.
3. Employees are responsible for ensuring that paper records are destroyed securely, ensuring that the confidential waste disposal system within the Hospice is used.
4. Guidance can be obtained from the Deputy Chief Executive/Director of Information Governance regarding the safe disposal of any IT equipment or portable storage media.
5. Employees must not disclose personal data without authorisation or agreement from the Deputy Chief Executive/Director of Information Governance, in line with the Disclosure/Provision of Information Policy & Procedure.

5.2 Employees Checklist for Recording Data

a. Do you really need to record the information?
b. Is the information 'standard' or is it 'sensitive'?
c. If it is sensitive, do you have the data subject's express consent?
d. Has the individual or data subject been told that this type of data will be processed?
e. Are you authorised to collect/store/process the data?
f. If yes, have you checked with the data subject that the data is accurate?
g. Are you sure that the data is secure?

h. If you do not have the data subject's consent to process, are you satisfied that it is in their best interests to collect and retain the data?
i. How long do you need to keep the data for, and what is the mechanism for review/destruction?

5.3 Service Users Confidential Health Information

Service users confidentiality health information is collected from service users in confidence and attracts a common law duty of confidence until it has been effectively anonymised. This legal duty prohibits information use and disclosure without consent – effectively providing individuals with a degree of control over who sees information they provide in confidence. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification. On admission and/or on first contact with the service for a particular matter, all service users should be asked which relatives, friends or carers they wish to receive information regarding treatment and progress, and those they specifically do not give permission to receive information. This information must be recorded in the clinical records. In cases where relatives have been heavily involved in service users care, the service users must be explicitly asked as to what level these relatives can be kept informed. This is particularly important in cases where relatives are requesting information on the service users's condition, perhaps before the service user has been informed.

5.4 Exemptions to Confidentiality

In certain circumstances personal information may be disclosed and guidance is below. However it is vital in each case that staff make an assessment of the need to disclose the information and document that the information has been released to whom and for what reason. If they are in any doubt, they should seek advice from the Deputy Chief Executive/Director of Information Governance/Caldicott Guardian.

5.4.1 Disclosing Information against the Service Users Wishes

The responsibility to withhold or disclose information without the data subject's consent lies with the Senior Manager Clinical Services or Senior Clinician (i.e. Consultant) involved at the time and cannot be delegated. Circumstances where the subject's right to confidentiality may be overridden are rare. Examples of these situations are:

- Where the subject's life may be in danger, or cases in which s/he may not be capable of forming an appropriate decision
- Where there is serious danger to other people, where the rights of others may supersede those of the subject, for example a risk to children or the serious misuse of drugs
- Where there is a serious threat to the healthcare professional or other staff
- Where there is a serious threat to the community
- In other exceptional circumstances, based on professional consideration and consultation.

The following are examples where disclosure without consent is required:

- Births and deaths - National Health Service Act 1977
- Notifiable communicable diseases - Public Health (Control of Diseases) Act 1984 15 SH IG 18 Data Protection & Confidentiality Policy Version 6 April 2019
- Poisonings and serious accidents at the work place - Health & Safety at Work Act 1974

- Terminations - Abortion Regulations 1991
- Child abuse - Children's Act 1989 and The Protection of Children Act 1999
- Drug Addicts - Drugs (Notification of Supply to Addicts) Regulations 1973
- Road traffic accidents - Road Traffic Act 1988
- Prevention/detection of a serious crime e.g. terrorism, murder - The Crime and Disorder Act 1998

If in doubt, staff should seek guidance, in confidence, from the Senior Manager Clinical Services or Senior Clinician (i.e. Consulatant) or the Deputy Chief Executive/ Information Governance Manager/Caldicott Guardian.

5.4.2 Non–Disclosure of personal information contained in a health record

An individual requesting access to their health records may be refused access to parts of the information if an appropriate clinician deems exposure to that information could cause physical or mental harm to the data subject or a third party. Clinicians should be prepared to justify their reasons in a court of law if necessary. In all cases reasons for nondisclosure must be documented. Where access would disclose information relating to or provided by a third party, consent for release must be sought from the third party concerned, unless that third party is a health professional who had provided the information as part of their duty of care. Where the third party does not consent, the information may be disclosed provided the identity of the third party is not revealed. The Information Commissioner's Code of Practice suggests that this might be done by omitting names and identifying particulars from the records. Care should be taken to ensure that the information if released is genuinely anonymous.

6.0 DATA PROTECTION IMPACT ASSESSMENT PROCEDURE AND TEMPLATE

All projects and processes that involve processing personal information or intrusive technologies give rise to privacy issues and concerns. To enable the Hospice to address the privacy concerns and risks the GDPR/DPA 18 requires a Data Protection Impact Assessment (DPIA) be completed, and signed off by the Deputy Chief Executive/Director of Information Governance (Appendix B).

7.0 GLOSSARY OF TERMS

7.1 Data

Any information which will be processed or used on or by a computerised system, additionally it also includes information contained within a "relevant filing system" of information. Data can therefore be written, tape, photographic or digital.

7.2 Personal Data

Personal data means data which relates to a living individual who can be identified:

a. from that data
b. from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller; and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

7.3 Data Subject

The person who is the subject of the "personal data".

7.4 Sensitive Personal Data

Categories of sensitive personal data, namely, personal data consisting of information as to:

a. the racial or ethnic origin of the data subject,
b. their political opinions,
c. their religious beliefs or other beliefs of a similar nature,
d. whether they are a member of a trade union,
e. their physical or mental health or condition,
f. their sexual life,
g. the commission or alleged commission by them of any offence,
h. any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

7.5 Data Controller

A person who determines the purposes for which, and the manner in which, any personal data are, or are to be, processed.

The Deputy Chief Executive/Director of Information Governance is the Data Controller for Alice House Hospice's data.

7.6 Data Processor

Any person (other than an employee of the data controller) who processes data on behalf of the data controller. The data controller retains responsibility for the actions of the data processor.

The Hospice processes data using the following third party software:

- SystmOne Hospital Palliative Care Module.
- Donorflex & Donorflex Lottery
- Software Medical Informatics (Staff.Care, eRostering and iPlanner)
- Sage 50 Accounts

7.7 Processing

Covers almost anything which is done with or to the data, including:

- obtaining data.
- recording or entering data onto the files.
- holding data or keeping it on file without doing anything to it or with it.
- organising, altering or adapting data in any way.
- retrieving, consulting or otherwise using the data.
- disclosing data either by giving it out, by sending it on email, or simply by making it available.
- combining data with other information.
- erasing or destroying data.

7.8 Consent

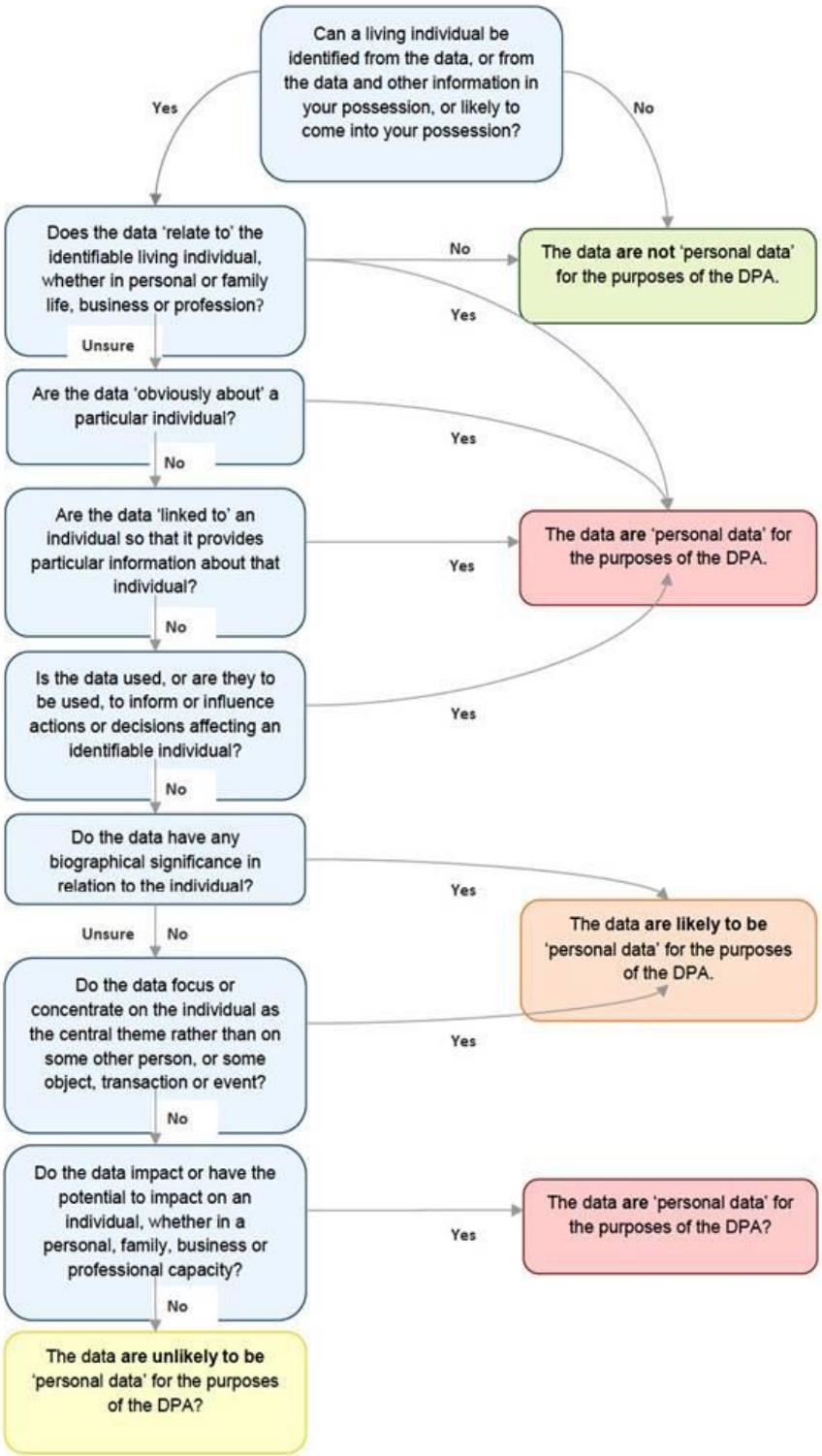
The European Data Protection Directive defines this as - any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. Consent can be withdrawn after it has been given. Where data is "sensitive", express consent must be given for processing this data.

7.9 Recipient

Under GDPR a recipient is defined as any person to who the data are disclosed, including any person to whom they are disclosed in the course of processing the data for the Data Controller (e.g. an employee of the data controller, a data processor or employee of the data processor).

APPENDIX A – PERSONAL DATA FLOWCHART

The following flow chart can be used by staff to help assess when certain kinds of data may or may not constitute Personal Data.



APPENDIX B – DATA PROTECTION IMPACT ASSESSMENT (DPIA) V1.0

DPIA Relating to: Business Function and Purpose of Processing	Reference

We must conduct a Data Protection Impact Assessment because:	
This is a new project, activity or workflow.	
This project, activity or workflow will involve the collection of new information about individuals.	
This project, activity or workflow will require individuals to provide personal or sensitive information.	
This project, activity or workflow will result in disclosure of information to organisations or individuals who have not previously had routine access to this information.	
This project, activity or workflow involves using new technology which may be perceived as being privacy intrusive.	
This project, activity or workflow will result in you making decisions or taking action against individuals in ways which can have a significant impact upon them.	
This project, activity or workflow is likely to raise privacy concerns or expectations due to the kind of information used about individuals.	
This project, activity or workflow will require us to contact individuals in ways which they may find intrusive.	

Describe how this activity is carried out – how is data shared or transferred between organisations?

What risks can be identified with this activity?				
Risk	**Description of Risk**	**Likelihood**	**Impact**	**Score**
1				
2				
3				
4				

Unacceptable Risks requiring action			
Risk	**Solution**	**Resulting Score**	**Re-Evaluation**
1			
2			
3			
4			
Are the risks detailed above acceptable?		YES	NO

PIA carried out by		Date	

Confirmation that risk reduction measures have been implemented where applicable		Date	

Likelihood	**5**						
	4						
	3						
	2						
	1						
		0	**1**	**2**	**3**	**4**	**5**
	Impact						

Risk Level	From	To	GDPR Assessment
High	15	25	Highest Unacceptable Risk
Medium	4	14	Unacceptable Risk
Low	1	3	Acceptable Risk
Zero	0	0	No Risk