G2 – Confidentiality

Summary	Organisational approach to confidentiality.
Document reference, eg, G41	G2 Policy
Applies to	All North Yorkshire Hospice Care staff
Author	Chief Executive
Additional NYHC staff who have contributed	
Scrutiny group(s) who have seen this document	LT BOT
Ratified by	BOT
Date of ratification	02/02/2022
Equality Impact Assessment	
Data Protection Impact Assessment	
Version	
Available on	T Drive Relias
Related organisational documents	
Date of implementation	February 2022
Date of next formal review	February 2024

Document Control

Date	Version	Action	Amendments

1. Introduction

1.1 Policy scope

This policy covers all work and services carried out by North Yorkshire Hospice Care (NYHC) a registered charity in England and Wales (518905). All staff and volunteers (where appropriate) operating its family of services, including Herriot Hospice Homecare, Just 'B', Saint Michael's Hospice and Talking Spaces, must therefore comply with the contents below. Throughout this document North Yorkshire Hospice Care and its family of services are referred to as 'we' 'us' 'our' for clarity and consistency.

1.2 Purpose of organisation

The purpose of our services is wide ranging, from end of life services to bereavement support and counselling.

2. Policy

It is our policy to ensure the General Principles stated in the following document are maintained to the highest possible standards, and that all staff are fully aware of the consequences should a breach of confidentiality occur.

3.General Principles

A duty of confidentiality arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. The relationship between patient and clinician is a clear example of this principle. The relationship between some donors and fundraising may be another.

Confidentiality is a legal obligation, established by case law and within professional codes of conduct of, for example, the General Medical Council, the Nurses and Midwifery Council and British Association of Counsellors and Psychotherapists. It is a specific requirement of all who work with and for us to agree to and sign a confidentiality statement. This includes, but is not restricted to, staff, volunteers, students and those working for us under service level agreements.

Patient and/or client information provided in confidence should not be used or disclosed in a way that might identify a patient and/or client without his or her consent, and sufficient assurances should be given to satisfy users that this principle is adhered to.

The NHS Confidentiality Model

It is our policy to follow the NHS model, which provides a professional approach in which the four main requirements are to:

- **Protect** patient information

- **Inform** patients about the need to share information within clinical teams

- **Provide choice** patients to decide whether their information can be disclosed or used in particular ways

- **Improve standards** wherever possible by heightened staff awareness and freedom to report potential breaches of confidentiality

4. Confidentiality

Multi-disciplinary Teams:

- The principle of sharing information within the team is necessary for its function but should be on a "need to know" basis and should remain confidential within the team. This applies to non-clinical members of the team and to volunteers as well as health professionals, even after the death of a patient.
- Notes and minutes from MDT meetings should be treated as confidential clinical information.
- Information used for audit and research should be anonymised whenever possible, any disclosure of personal information requires informed consent.
- Personal information for publication in the press or in our literature should not be used without informed consent.

In provision of care and support:

- Vigilance must be maintained to preserve confidentiality when patients or carers or clients are already known to members of staff or when members of staff become patients or clients of ours.
- Care must be taken to ensure that patient/carer/client information must not become the subject of gossip or comment outside the clinical or support services' environment.
- Staff should be careful to avoid discussion of clinical or support services' information in areas where conversations may be overheard, even within our organisation. Audio-privacy should be maintained whenever possible.
- The need for peer support and debriefing in stressful situations should not compromise confidentiality.
- Giving information on request to relatives and friends is a sensitive area, but it should be understood that the permission of the patient/client is required for any disclosure, however close the relationship. Collusion with relatives to withhold information from a patient may also breach this principle and requires the exercise of professional judgement.

- The duty of confidentiality persists after death. Information sharing in this scenario is governed by the Access to HealthCare Records Act 1990 and, unless covered in the scenarios outlined below, should be discussed with the Caldicott Guardian for the organisation.
- Information on the death certificate (name, date and place of death, cause of death) is published and therefore in the public domain once the death has been recorded and is therefore then not confidential.
- In addition, professional body (BMA) guidance states that the clinician can use their discretion on sharing information with relatives to help them understand the person's final illness and/or last days.

Handling clinical information

- All written personal clinical records must be stored securely and in an area accessible only to those staff who need access. Confidential papers should be protected inside folders or envelopes while in transit.
- Temporary notes containing patient details must be carefully disposed of when no longer in use, ideally by shredding.
- Systems to protect electronic patient data must be secure, with data accessible only to the relevant staff and password protected where possible.
- Use of a fax machine requires care to ensure that the information reaches the intended destination
- Email should only be used when there is secure encryption of data, at time of writing for this reason its use for transfer of clinical data is not recommended.

Handling client services information (Just 'B', Volunteer Visitors and Patient and Family Support)

- All client information must be held electronically and accessible only to relevant staff and volunteers. Systems to protect electronic client data must be secure and password protected where possible. Any paperwork completed during a session must be stored securely in a locked cabinet until no longer needed, at which point it must be carefully disposed of in the confidential waste for shredding.
- Confidential papers should be protected inside folders or envelopes while in transit internally and in lockable folders while in transit off site.
- All client information must be treated as confidential and should not be disclosed unless permission is received from the subject or is required by a statutory body.
- Email should only be used when there is secure encryption of data, at time of writing for this reason its use for transfer of client data is not recommended.

Information relating to Staff, Volunteers and Supporters

- All non-clinical personal information must also be treated as confidential and should not be disclosed unless permission is received

from the subject or is required by a statutory body. The sharing of addresses and telephone numbers is restricted to members of the leadership team only, unless there are concerns for the safety of a member of staff or volunteer. Information must be stored securely and must not be left in general view. Destruction of information must take place securely and records kept.

- Electronic systems must be secure and password protected.
- NYHC will not sell or swap personal supporter data and will only use it in accordance with our information notice (see section on Who we share your information with).
- All supporter information must be treated as confidential and should only be used in accordance with our information notice, for example where permission is received from the supporter or is required by a statutory body.
- All written personal supporter records must be stored securely, in an area accessible only to those staff who need access.
- Confidential papers should be protected inside folders or envelopes while in transit.
- Systems to protect electronic supporter data must be secure, with data accessible only to the relevant staff and password protected where possible.
- Temporary notes containing supporter details must be carefully disposed of in the confidential waste for shredding.

Breaches of confidentiality, whether careless or deliberate can have serious consequences, and should be reported to a member of the Leadership Team as soon as possible after the event. All staff are encouraged to highlight areas of risk as they become aware of them and report them to the members of the team with responsibility for information governance.

The members of staff who have been allocated smartcards must follow the terms and conditions relating to their use and not lend or pass their cards to other people. Any breach of the terms and conditions will be regarded as a breach of confidentiality.

All breaches of confidentiality will be considered under the disciplinary procedures and may lead to dismissal.