Rotherham Safeguarding Adults Board

Policy for Managing Concerns and Allegations around People in Positions of Trust (PiPoT) with Adults who have Care and Support Needs

Published: June 2020

Review: June 2021

Rotherham
Safeguarding Adults

Table of Contents

Rotherham's Safeguarding Adults Board (RSAB) is multi-agency partnerships made up of a wide range of statutory, independent and voluntary agencies and organisations. These all work together to keep adults, particularly those who are more vulnerable, safe from the risk of abuse, harm or exploitation.

Tele: 01709 822330 or Email: singlepointofaccess@rotherham.gov.uk
Web: rsab.org.uk

1.0 Introduction

This document provides an overarching policy for Rotherham which has been ratified by the Rotherham Safeguarding Adults Board and all partners.

Under the Care Act 2014 Statutory Guidance ("the Guidance") Safeguarding Adults Boards need to establish and agree a framework and process for how allegations against people working with adults with care and support needs (for example, people in positions of trust – hereafter referred to as "PiPoT" should be notified and responded to.

Whilst the focus of safeguarding adults work is to safeguard one or more identified adults with care and support needs, there are occasions when incidents are reported that do not involve an adult at risk, but indicate, nevertheless, that a risk may be posed to adults at risk by a person in a position of trust.

The management of any issues relating to PiPoT are governed by the Data Protection Act 2018 and the principles outlined in the Act.

The Care Act 2014 requires that partner agencies and their commissioners of services should have clear recordings and information sharing guidance, set explicit timescales for action and are aware of the need to preserve evidence. This policy draws upon existing relevant statutory provision.

Six key principles underpin all adult safeguarding work:-

Empowerment	People being supported and encouraged to make their own decisions and informed consent
Prevention	It is better to take action before harm occurs
Proportionality	The least intrusive response appropriate to the risk presented
Protection	Support and representation for those in greatest need
Partnership	Local solutions through services working with their communities. Communities have a part to play in preventing detecting and reporting neglect and abuse
Accountability	Accountability and transparency in delivering safeguarding

Situations covered by the guidance

Action may need to be taken in respect of a PiPoT in the following circumstances where there are concerns or evidence that:

- The person has harmed an adult or a child in a professional role
- The person has harmed an adult or a child in a personal relationship
- The person has harmed an adult or a child in some other role of capacity

And:

- It is believed that the above poses a current of continuing risk in the person's current role of responsibility (whether paid or unpaid)

Concerns may be raised through a variety of processes including:

- Criminal investigations
- Section 42 Enquires under the Care Act 2014
- Children's safeguarding enquiries
- Disciplinary investigations
- Regulatory action
- Reports from the public

This policy gives guidance about the following considerations: information sharing; employer responsibilities; risk assessments; employee rights etc. The Data Protection Act 2018, European General Data Protection Regulation (2018) and Human Rights Act 1998 must be taken into account within this process.

Each agency is responsible for the management and handling of its own information and is also responsible for issues of disclosure. Each agency should have a designated lead officer for managing issues relating to positions of trust.

This policy relates to those instances where a relevant agency is alerted to information that may affect the suitability of a paid person, or volunteer to work with an adult(s) at risk. The concern may be related to an issue both within and outside work. The alleged victim, in such circumstances, does not have to be an adult at risk, for example, it could be the PiPoT's partner, another adult or a child. This document refers to when there is an allegation which may not directly involve an adult at risk but could have risk implications in relation to the employment or volunteer work of a person in a position of trust (PiPoT).

What is excluded from this policy?
If an allegation is made that does concern the actions of a paid person, or volunteer which related to alleged abuse or neglect of a person with care and support needs and this amounts to a safeguarding enquiry, then such an allegation should be dealt with by following the local adult safeguarding policies and procedures. Such procedures include directions about how such allegations are referred and investigated (see South Yorkshire Principles and Approach to Safeguarding).

Under the Guidance, safeguarding is not a substitute for:

- Providers' responsibilities to provide safe and high quality care and support
- Commissioners regularly assuring themselves of the safety and effectiveness of commissioned services
- The Care Quality Commission (CQC) ensuring that regulated providers comply with the fundamental standards of care or by taking enforcement action; and
- The core duties of the police to prevent and detect crime and protect life and

property

Therefore, careful consideration should be given to distinguish clearly between:

- A complaint about a paid person, or volunteer
- Allegations raised about the quality of practice provided by the person in a position of trust, that do not meet the criteria for a safeguarding enquiry

Other Professional Regulatory bodies and their procedures should be used to recognise, respond to and resolve these issues. e.g. Nursing Midwifery Council (NMC), Social work England (SWE), Health and Care Professionals Council HCPC)

2.0 Responsibilities

Rotherham Safeguarding Adults Board (RSAB)

Each partner agency, in their self-assessment submission to the RSAB, will be required to provide assurance that arrangements to deal with allegations against a PiPoT within their organisation are adequate and are functioning effectively. All partners will be required to share their PiPoT policy with the RSAB. The RSAB will, in turn, maintain oversight of whether these arrangements are considered to be working effectively between, and across partner agencies in the local authority area.

Local Authority

Under section 6 of the Care Act 2014, the Local Authority has a duty to cooperate with each of its relevant partners, and each relevant partner must cooperate with the Local Authority in respect of their respective functions including in relation to:

- Adults with needs for care and support
- Carers with needs for support

Section 6(7) of the Care Act 2014 sets out a list of the “relevant partners”.

As the lead agency for Adult Safeguarding Local Authorities are often in receipt of sensitive information regarding PiPoT. Each local authority will have a lead officer who can be contacted by internal and external colleagues about issues posed by the behavior, or alleged behavior of a PiPoT, this will be the Safeguarding Operational Manager.

The lead officer will consider information that is shared with them and will normally encourage the agencies that are the Data Controllers (page 6) to make decisions regarding disclosure. In a smaller number of cases the agencies may not be willing or able to decide on whether disclosure is appropriate and, in this situation, the RSAB may need to implement the external escalation policy.

There will be some circumstances where the information is not clearly in the possession of any Data Controller, or where the information is provided by a member of the public. As RSAB is not an independent organisation registered with the Information Commissioner’s

Office (www.ico.org.uk) then RMBC would be the overall lead organisation (in terms of lead data controller). This is because the RSAB sits within RMBC as the 'host' organisation. In these cases Rotherham MBC will assume the role of lead Data Controller and coordinate a reply with the involvement and support of relevant member organisations. In certain cases where the paid person or volunteer has links to several organisations or where there is believed to be a risk to adults in several settings it may be necessary for the Local Authority or lead agency to convene a meeting to consider the information that is held and to make a decision regarding disclosure and/or further action. In cases where two or more member organisations are involved then Rotherham Metropolitan Borough Council will act as the lead organisation and coordinate a reply, with the involvement and support of the relevant member organisations.

Agencies and Voluntary Organisations

Agencies and voluntary organisations should have clear and accessible policy and procedures in place setting out the PiPoT process. These should determine who should undertake an investigation and include timescales for investigation and include how support and advice will be made available to individuals against whom allegations have been made. Any allegations against people who work with adults, should be reported immediately to a senior manager within the organisation. Employers, student bodies and voluntary organisations should have their own source of advice (including legal advice, if felt appropriate) in place for dealing with such concerns.

Where such concerns are raised about someone who works with adults with care and support needs, it will be necessary for the employer (or student body or voluntary organisation) to assess any potential risk to adults with care and support needs who use their services and, if necessary, to take action to safeguarding those adults.

Examples of such concerns could include allegations that relate to a person who works with adults with care and support needs who has:

- Behaved in a way that has harmed, or may have harmed an adult or child
- Possibly committed a criminal offence against, or related to, an adult or child
- Behaved towards an adult or child in a way that indicates they may pose a risk of harm to adults with care and support needs

Children

When a person's conduct towards an adult may impact on their suitability to work with, or continue to work with children, this must be referred to the Local Authority Designated Officer (LADO). In any case where a person is believed to pose a risk to children the information must be immediately shared with the Local Authority Designated Officer (LADO) for that Local Authority.
http://www.rscp.org.uk/homepage/73/local_authority_designated_officer

Where concerns have been identified about their practice and they are a parent/carer for children, then consideration by the Data Controller should be given to whether a referral to Children's Services is required.

Data Controller

If an partner agency is in receipt of information, that gives cause for concern about a person in a position of trust, then that agency should give careful consideration as to whether they

should share the information with the person's employers, (or student body or voluntary organisation), to enable them to conduct an effective risk assessment. The receiving organisation becomes the **Data Controller** as defined by the Data Protection Act 2018 and GDPR; Article 4 (please refer to Section 4.0 Legal Framework).

Partner agencies and the service providers they commission, are individually responsible for ensuring that information relating to PiPoT concerns, are shared and escalated outside of their organisation in circumstances where this is required. Such sharing of information must be lawful, proportionate and appropriate. Organisations are responsible for making the judgment that this is the case in every instance when they are the **Data Controller**.

As RSAB is not an independent organisation registered with the Information Commissioner's Office (www.ico.org.uk) then RMBC would be the overall lead organisation (in terms of data controller). This is in instances where: i) there is no clear lead, and/or, ii) two or more of the member organisations are involved and a coordinated reply is required, iii) a request is made directly to the body RSAB. This is because the RSAB sits within RMBC as the 'host' organisation.

If, following an investigation a PiPoT is removed, by either dismissal or permanent redeployment, to a non-regulated activity, because they pose a risk of harm to adults with care and support needs, (or would have, had the person not left first), then the employer (or student body or voluntary organisation), has a legal duty to refer the person to the Disclosure and Barring Service (DBS). ***It is an offence to fail to make a referral without good reason.*** In addition, where appropriate, employers should report workers to the statutory and other bodies, responsible for professional regulation such as the Health and Care Professions Council, General Medical Council, Nursing and Midwifery Council and Social Work England.

If a person subject to a PiPoT investigation, attempts to leave employment by resigning in an effort to avoid the investigation or disciplinary process, the employer (or student body or voluntary organisation), is entitled **not** to accept that resignation and conclude whatever process has been utilised with the evidence before them. This is an employment issue for each organization and legal advice should be sought, if felt appropriate. If the investigation outcome warrants it, the employer may consider dismissal of the employee or volunteer instead and make a referral to the DBS. This would also be the case where the person intends to take up legitimate employment or a course of study.

3.0 Information Sharing

The Guidance sets out that decisions on sharing information must be justifiable and proportionate, based on the potential or actual harm to adults or children at risk and the rationale for decision-making should always be recorded. Disclosure of confidential information without consent is to be considered on the basis of proportionality and information can be disclosed only if there is a pressing need for that disclosure.

This means:-

- The legitimate aim in question must be sufficiently important to justify the interference

- The measures taken to achieve the legitimate aim must be rationally connected to it
- The means used to impair the right must be no more than necessary to accomplish the objective
- A fair balance must be struck between the rights of the individual and the interests of the community, this requires a careful assessment of the severity and consequences of the interface

When sharing information about adults, children and young people at risk between agencies it should only be shared:

- Where relevant and necessary, not simply all of the information held
- With the relevant people who need some or all of the information
- When there is a specific need for the information to be shared at that time

Keep the following in mind:-

Remember that the General Data Protection Regulation (GDPR) and Caldicott guidance is not a barrier to sharing information but provides a framework to ensure that the personal information about living persons is shared appropriately.

- Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared and see their agreement, unless it is unsafe to do so.
- Seek advice if you are in any doubt, without disclosing the identity of the person where possible.
- Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if in your judgement that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.
- Consider safety and wellbeing: base your information-sharing decisions on considerations of the safety and wellbeing of the person and others who may be affected by their actions.
- Necessary, proportionate, relevant, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it is accurate and up to date, is shared in a timely fashion and is shared securely.
- Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Timescales

This policy applies whether the allegation or incident is current or historical.

Required Action
The initial responsibility lies with each agency to determine whether it can identify and address issues internally, using its standard processes. All agencies are reminded of their legal duty to make referrals to the Disclosure and Barring Service (DBS) when a person is dismissed or had left when they would have been dismissed for harming a child or an adult with care and support needs.

All agencies must consider whether they have information that may require disclosure to another agency and, as the primary data controller, the decision lies with them. Where an agency decides that information does need to be disclosed to another agency it should, where practicable, give the alleged PiPoT the opportunity to disclose the information in the first instance.

If the person declines to share the information the agency must decide whether it is necessary and proportionate for this information to be shared. The information shared should be as little as necessary in the circumstances and the person should be made aware of the decision to disclose the information.

Recording
Recording of discussions, decisions and disclosures is essential and each agency must ensure that it has a process for recording this information. Any recording must be compliant with the requirements and principles of the Data Protection Act 2018.

Recording is likely to be subject to access requests unless there are strong grounds for this to be denied and internal processes should be as transparent and inclusive for the person involved as is possible.

Agencies must be clear regarding their retention policy schedule of any records that are kept and must be prepared to remove and destroy any records for which there is no longer any reasonable need to retain.

4.0 Legal Framework

Both the Data Protection Act 2018 and GDPR define the following: Data Subject means an individual who is the subject of personal data. In other words, the data subject is the individual whom particular personal data is about. The Act does not count, as a data subject, an individual who has died or who cannot be identified or distinguished from others.

Data Controller means……. a person who (either alone or jointly or in common with other persons) determines the purposes for which and the way any personal data are, or are to be, processed.

In other words, the Data Controller is the organisation or individual who holds the PiPoT's personal data. The Data Controller is considered to be the owner of the information and has responsibility for taking appropriate action i.e. risk assess and decide whether to disclosure the information.

It is the Data Controller that must exercise control over the processing and carry data protection responsibility for it. The Data Controller must be a "person" recognised in law,

that is to say:

- Individuals
- Organisations
- 0ther corporate and unincorporated bodies of persons

A Data Controller- will usually be an organisation, but can be an individual, for example a self-employed consultant. An individual given responsibility for data protection in an organisation will be acting on behalf of the organisation; the Data Controller.

The term Data Controllers is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term in common applies where two or more persons, share a pool of personal data that they process independently of each other.

Data Controllers must ensure that any processing of personal data, for which they are responsible complies with the Data Protection Act 2018. Failure to do so risks enforcement action, even prosecution and compensation claims from individuals.

Data Processor - in relation to personal data, means any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller.

The Data Protection Act 2018 and the GDPR (please refer to Appendix 1) requires anyone handling personal information to comply with the principles set out in the Acts:

- The information processed must be fair and lawful
- Personal data must be kept in a secure and confidential place.

The Information Commissioners Office (ICO) upholds information rights in the public interest. Further information about the law relating to data use/control can be found on their website.

The Crime and Disorder Act (1998) states any person may disclose information to a relevant authority under Section 115 of the Act:

"Where disclosure is necessary or expedient for the purposes of the Act (reduction and prevention of crime and disorder)"

The Human Rights Act (1998) – The principles set out in the Human Rights Act must also be taken into account within this framework in particular the following:

Article 6 – The right to a fair trial; this applies to both criminal and civil cases against them…… the person is presumed innocent until proven guilty according to the law, and has certain guaranteed rights to defend themselves.

Article 7 – A person who claims that a public authority has acted or proposes to act in a way which is unlawful by section 6(1) may a) bring proceedings against the local authority under this act in the appropriate court or tribunal or b) rely on the convention rights or rights concerned in any legal proceedings.

Article 8 – The right to respect for private and family life.

APPENDIX 1: Data Protection Act 2018 and General Data Protection Regulations GDPR Overview

The contents of this Appendix are meant as a general guide and should not be relied upon as a substitute for legal advice. If in doubt you should consult with a lawyer.

Both regulate the use of "personal data". To understand what personal data means, we need to first look at how the Act defines the word "data".

Data means information which:

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose
(b) is recorded with the intention that it should be processed by means of such equipment
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system
(d) does not fall within A, B or C above but forms part of an accessible record as defined by Section 68, or
(e) is recorded information held by a public authority and does not fall within any of paragraphs a-d above

What is personal data?
Personal data means data which relate to a living individual who can be identified:

(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller

…and involves 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.

Sensitive personal data, also known as special category data in Article 9 of the GDPR, means personal data consisting of information as to:

(a) the racial or ethnic origin of the data subject
(b) His/her political opinions
(c) His/her religious beliefs or other beliefs of a similar nature
(d) whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
(e) His/her physical or mental health condition
(f) His/her sexual orientation
(g) the commission or alleged commission by him/her of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

The Act regulates the "processing" of personal data. Processing in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –

(a) organisation, adaptation or alteration of the information or data
(b) retrieval, consultation or use of the information or data
(c) disclosure of the information or data by transmission, dissemination or otherwise making available
(d) alignment, combination, blocking, erasure or destruction of the information or data.

Chapter 2of the Data Protection Act 2018 sets out the 6 data protection principles as a list of the following 'requirements' as the general duty of the Data Controller:-

1. that processing be lawful and fair
2. the purposes of processing be specific, explicit and legitimate
3. personal data be adequate, relevant and not excessive
4. Personal data be accurate and kept up to date
5. Personal data be kept for no longer than is necessary
6. Personal data be processed in a secure manner

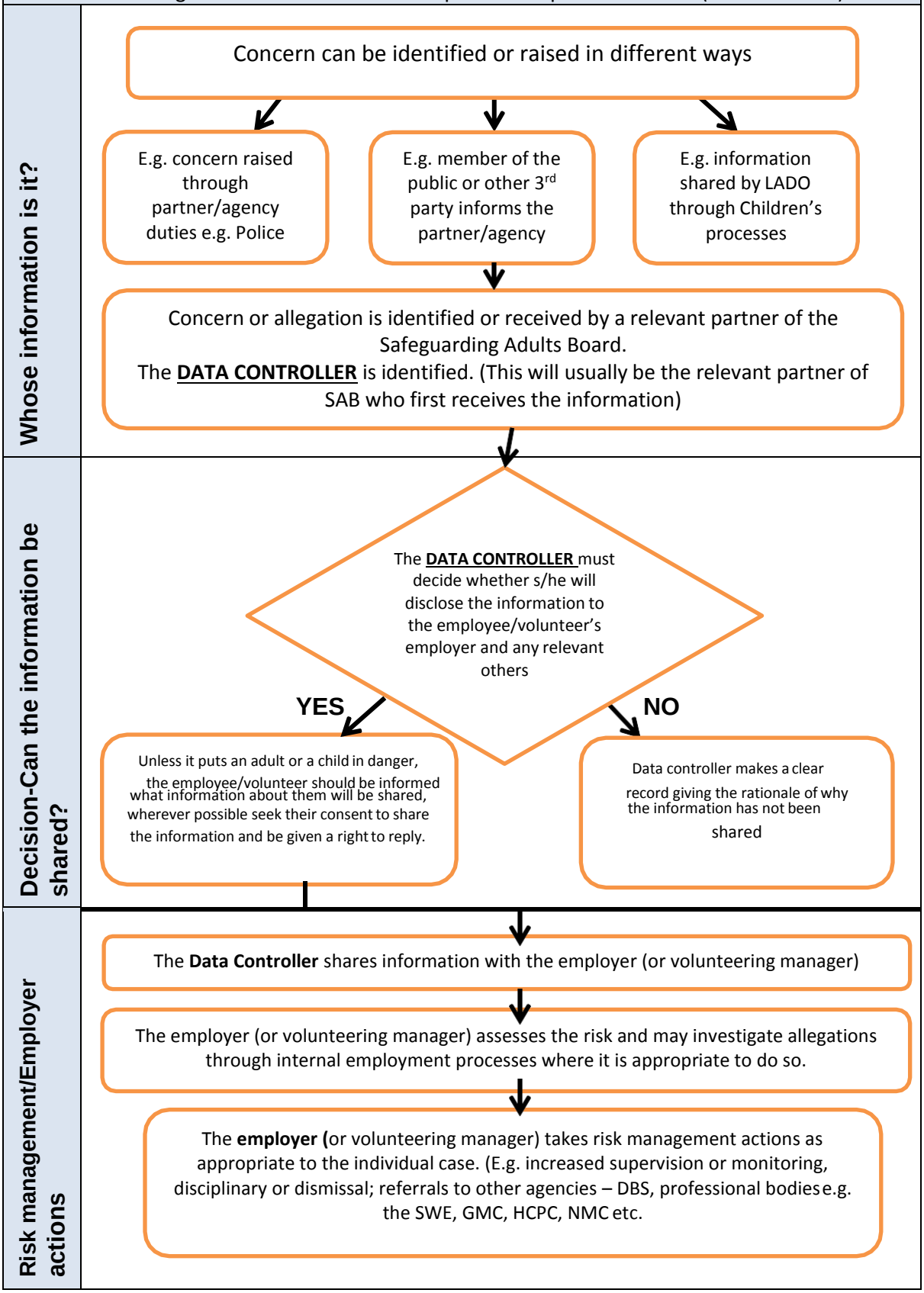
A Data Controller is a person, company or other body that determines the purpose and means of personal data processing (this can be determined alone, or jointly with another person/company/body).This means that where an organisation is required by law to process personal data, it must retain Data Responsibility for the processing. It cannot negate its responsibility by 'handing over' responsibility for the processing to another Data Controller or Data Processor. Although a request can be made to them to carry out certain aspects of the processing of the information, overall responsibility remains with the organisation with the statutory responsibility to carry out the processing.

To determine whether you are a Data Controller you need to ascertain which organisation decides:

- to collect the personal data in the first place and the legal basis for doing so
- which items of personal data to collect, i.e. the content of the data
- the purpose or purposes the data are to be used for
- which individuals to collect data about
- whether to disclose the data, and if so, who to
- whether subject access and other individuals' rights apply i.e. the application of exemptions; and
- how long to retain the data or whether to make non-routine amendments to the data.

APPENDIX 2: Managing Concerns and Allegations against People who work with Adults with Care and Support Needs Flowchart

Process for dealing with the concern about the person in a position of trust (PiPoT concern)



REFERENCES
Information Commissioner's Office – Guide to the Data Protection Act For further information visit: https://ico.org.uk/for-organisations/guide-to-the-general-data- protection-regulation-gdpr/principles/ Gov.UK guide to GDPR: https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation Caldicott Guidance: www.igt.hscic.gov.uk/Caldicott2Principles.aspx Rotherham Adult Position of Trust Framework: A Framework and Process for responding to allegations and concerns against people working with adults with care and support needs (2020)

GLOSSARY	
ADASS	Association of Directors of Adult Social Services
https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation	https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation
Data Controller	A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed
Data Subject	An individual who is the subject of personal data
Data Processor	In relation to personal data any person (other than an employee of the data controller), who processes the data on behalf of the data controller
PiPoT	Person in a Position of Trust
RSAB	Rotherham Safeguarding Adults Board
Partners	Partners of the Rotherham Safeguarding Adults Board