North West Policy for Managing Concerns around People in Positions of Trust with Adults who have Care and Support Needs

Version 5.3 June 2019

Contents

Information Sheet 3

Glossary 4

1.0 Introduction 5

2.0 Responsibilities 6

3.0 Information Sharing 8

4.0 Legal Framework 9

APPENDIX 1: Data Protection Act and GDPR Overview 11

APPENDIX 2: Managing Concerns and Allegations against People who work with Adults with Care and Support Needs Flowchart 14

REFERENCES 16

This policy has been developed and based upon the West Midlands 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 (2017)

Information Sheet

Title	North West Policy for Managing Concerns around People in Positions of Trust with Adults who have Care and Support Needs
Responsible Officer	ADASS North West Safeguarding Lead
Ratified By	
Ratification date	
Implementation date	1.3.2018
Review Period	Annual
Review Date	1.3.2020
Version Updates	V5.3 June 2019
Responsible Group	North West Safeguarding Leads Group

Glossary

ADASS	**Association of Directors of Adult Social Services**
DBS	**Disclosure & Barring Service**
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 position of trust**
SAB	**Safeguarding Adults Board**

1.0 Introduction

This document provides an overarching policy for the North West Region which has been ratified by the North West ADASS Regional Safeguarding Group. This should be read in conjunction with local Person in a Position of Trust (PiPoT) Guidance and existing local Safeguarding Adults Procedures and Practice Guidance.

The Care Act 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 builds upon existing relevant statutory provision. The guidance for 'Managing allegations against people in a position of Trust' is contained within section 14 of the Care and Support Statutory Guidance of the Care Act 2014. Other relevant legislation includes: Data Protection Act 2018/European General Data Protection Regulation 2018 [GDPR]; Human Rights Act 1998 and employment legislation.

As with all adult safeguarding work the six principles underpinning the Care Act 2014 should inform this area of activity:

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 safeguarding practice

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.

This policy relates to those instances where a relevant agency is alerted to information that may affect the suitability of a professional, or volunteer to work with an adult(s) at risk, where such information has originated from activity outside their professional or volunteer role and place of work. The alleged victim, in such circumstances, does not have to be an adult at risk, for example, it could be their partner or a child. This document refers to when there is an allegation which does not directly involve an adult at risk, but may 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 professional, or volunteer which relates 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 should include directions about how such allegations are referred and investigated.

Section 14 of the Care Act Care and Support Statutory Guidance states:

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
- 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 professional, or volunteer
- concerns 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 relevant bodies and their procedures should be used to recognise, respond to and resolve these issues.

2.0 Responsibilities

Safeguarding Adults Board

Safeguarding Adults Boards need to establish and agree a framework and process, for how concerns and allegations against people working with adults with care and support needs (i.e. those in positions of trust) should be notified and responded to. Whilst the focus on 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**

Each partner agency, in their annual assurance statement to the SAB, will be required to provide assurance that arrangements to deal with allegations against a person in a position of trust, within their organisation are adequate and are functioning effectively. The SAB 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. Appropriate cross organisational challenge should be possible as it is an important part of this process.

Local Authority

The Local Authority relevant partners, are set out in section 6 (7) of the Care Act 2014.

Pursuant to the Care Act 2014 there is a requirement that Safeguarding Adults Boards for local authorities, should establish and agree a framework and process for any organisation to respond to allegations against anyone, who works in either a paid or unpaid capacity with adults with care and support needs.

Partners

Employers, student bodies 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. Individuals should also be made aware of their rights under employment legislation and any internal disciplinary procedures.

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) 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). 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.

Concerns raised by local authority children teams

Where a concern has arisen following an assessment by the local authority children's teams, then they are the data controller, they must decide through their assessment whether the employing organisation is required to be informed in order to manage any risks**.**

Data Controller

If an organisation is in receipt of information, that gives cause for concern about a person in a position of trust, then that organisation 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**.

If, following an investigation a Person in a Position of Trust 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.*** If unsure contact the DBS for further advice. 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 and the Nursing and Midwifery Council.

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. If the investigation outcome warrants it, the employer can dismiss 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

Both the GDPR and the Data Protection Act 2018 [DPA2018] identify statutory obligations and gateways when sharing a data subject's information. In particular DPA 2018 Schedule 8 provides for the conditions to share information based on safeguarding and vital interests.

In all cases the sharing of information must be legal, 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.

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

- Where there is a legal justification for doing so
- where relevant and necessary, not simply all the information held
- with the relevant people who need all or some of the information
- when there is a specific need for the information to be shared at that time

Timescales

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

4.0 Legal Framework

Both the Data Protection Act 2018 and the 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. Whilst the legislation is no longer applicable once a data subject is deceased, a common law duty of confidentiality may result in certain restrictions being considered on a case by case basis.

Data Controller means 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.

In other words the Data Controller is the organisation or individual who first becomes aware of the allegation or concern. 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 disclosure to other bodies should be made.

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; and
- other corporate and unincorporated bodies of persons

Data Controllers will usually be organisations, but can be individuals, for example self-employed consultants. An individual given responsibility for data protection in an organisation will be acting on behalf of the organisation, which will be the Data Controller.

In relation to Data Controllers, the term jointly 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 act. 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. For 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 GDPR Overview

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 relates 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 data 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

The Data Protection Act 2018 and Article 5 of the GDPR lists the data protection principles in the following terms:

The first data protection principle

(1) The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.

(2) The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either:

(a) The data subject has given consent to the processing for that purpose, or

(b) The processing is necessary for the performance of a task carried out for that purpose by a competent authority.

(3) In addition, where the processing for any of the law enforcement purposes is sensitive processing, the processing is permitted only in the two cases set out in subsections (4) and (5).

(4) The first case is where

(a) The data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection (2)(a), and

(b) At the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(5) The second case is where

(a) The processing is strictly necessary for the law enforcement purpose,

(b) The processing meets at least one of the conditions in Schedule 8, and

(c) At the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

The second data protection principle

(1) The second data protection principle is that:

> (a) The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and
>
> (b) Personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected

The third data protection principle

The third data protection principle is that personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

The fourth data protection principle

(1) The fourth data protection principle is that:

> (a) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and
>
> (b) every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

The fifth data protection principle

(1) The fifth data protection principle is that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.

(2) Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes

The sixth data protection principle

The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

Section 6(2) of the Data Protection Act 2018 Chapter 2 GDPR says that:

Where personal data are processed only for purposes for which they are required by or under any enactment to be processed, the person on whom the obligation to process the data is imposed by or under that enactment is for the purposes of this Act, the data controller.

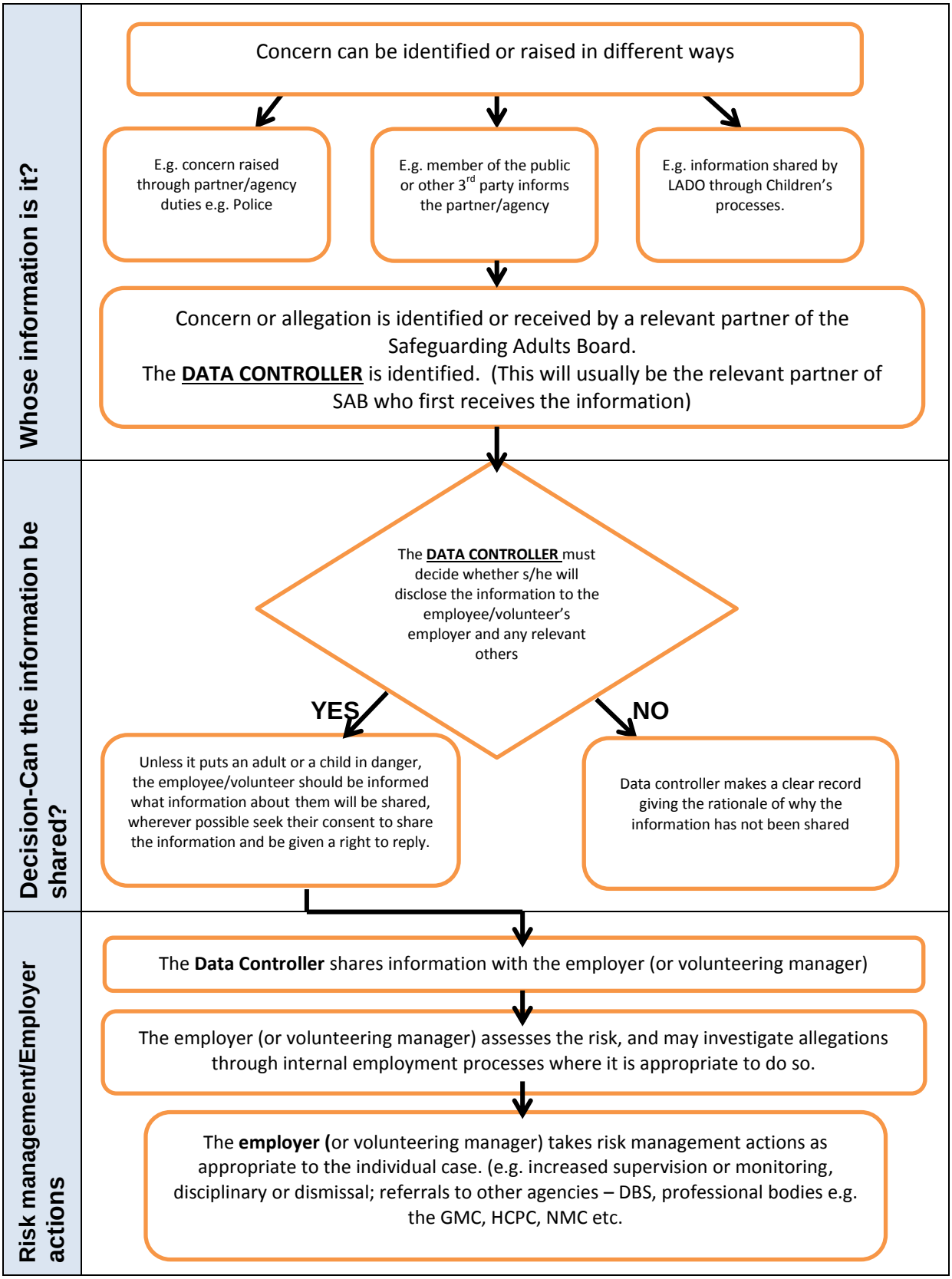
This means that where an organisation is required by law to process personal data, it must retain data controller responsibility for the processing. It cannot negate its responsibility by 'handing over' responsibility for the processing to another data controller or data processor. Although it could use either type of organisation to carry out certain aspects of the processing for it, 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

These are all decisions that can only be taken by the data controller as part of its overall control of the data processing operation.

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)


Whose information is it?
Concern can be identified or raised in different ways
E.g. concern raised through partner/agency duties e.g. Police
E.g. member of the public or other 3rd party informs the partner/agency
E.g. information shared by LADO through Children's processes.
Concern or allegation is identified or received by a relevant partner of the Safeguarding Adults Board.
The DATA CONTROLLER is identified. (This will usually be the relevant partner of SAB who first receives the information)
Decision-Can the information be shared?
The DATA CONTROLLER must decide whether s/he will disclose the information to the employee/volunteer's employer and any relevant others
YES
NO
Unless it puts an adult or a child in danger, the employee/volunteer should be informed what information about them will be shared, wherever possible seek their consent to share the information and be given a right to reply.
Data controller makes a clear record giving the rationale of why the information has not been shared
Risk management/Employer actions
The Data Controller shares information with the employer (or volunteering manager)
The employer (or volunteering manager) assesses the risk, and may investigate allegations through internal employment processes where it is appropriate to do so.
The employer (or volunteering manager) takes risk management actions as appropriate to the individual case. (e.g. increased supervision or monitoring, disciplinary or dismissal; referrals to other agencies – DBS, professional bodies e.g. the GMC, HCPC, NMC etc.

REFERENCES

Information Commissioner's Office – Data Controllers and Data Processors: What Difference is and What the Governance Implications are. Data Protection Act

Information Commissioner's Officer – Guide to the Data Protection Act

West Midlands 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 (2017)

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/