North Lincolnshire Safeguarding Adults Board

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

Document control

Date approved: February 2022

Review date: February 2024

Date	Version	Changes
22 February 2022	Version	Version approved.
1 February 2022	Draft 7	Final Draft
22 February 2022	Final	Review February 2024
19 December 2023	Final	Approved
12 April 2024	Update	P7 and P 16 New Safeguarding Adults Team email address

07 August 2024	Update	Appendix 5 PiPoT e-form link

Contents

1. Introduction

The purpose of this policy is to provide a framework for managing cases where allegations have been made against a person in a position of trust (PiPoT) and is focussed on the management of risk. It provides guidance to ensure appropriate actions are taken to manage allegations against people who work, either in a paid or unpaid capacity, with adults with care and support needs.

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

This policy is based on the Care Act 2014 which 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.

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 resented.
- **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 abuse and neglect.
- **Accountability** – accountability and transparency in safeguarding practice.

Where applicable this policy should be read in conjunction with 'Procedures for managing allegations against people who work with children', which is available at Managing Allegations Against People who work with children (northlincscmars.co.uk)

2. 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 whilst 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 or capacity.

And:

- It is believed that the above poses a current or 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 regarding the following considerations: information sharing; employer responsibilities; risk assessments and employee rights. The General Data Protection Regulation 2018 and Human Rights Act 1998 must **always** be considered within this process. This policy must also be read in conjunction with the North Lincolnshire Safeguarding Adults Board Multi-Agency Policy & Procedures.

This policy relates to those instances where a relevant agency is alerted to information that may affect the suitability of an employee, volunteer, or student 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 includes instances 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).

3. What is excluded from this policy?

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

Safeguarding is not a substitute for:

- Providers' responsibilities are to provide safe and high-quality care and support.
- Commissioners regularly assure themselves of the safety and effectiveness of commissioned services.
- The Care Quality Commission (CQC) ensures that regulated providers comply with the fundamental standards of care or by taking enforcement action.
- The core duties of the police are 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 does 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.

4. Information sharing and the legal framework.

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.

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.

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 seek 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.

4.1 Legal framework

The Data Protection Act 1998 and General Data Protection Regulations (GDPR) set out the key principles, rights, and obligations for most processing of personal data. Both define the following:

The Data Protection Act 1998 and GDPR

Data subject means an individual who is the subject of personal data.

In other words, the data subject is the individual whom 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 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 in the same organisation, who processes the data on behalf of the data controller.

Both The Data Protection Act 1998 and the GDPR 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.

Other relevant legislation to this policy can be found in appendix (1)

5. Responsibilities

5.1 North Lincolnshire Safeguarding Adults Board (NLSAB)

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 (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 will be required to provide assurance to the NLSAB that arrangements to deal with allegations against a person in a position of trust, within their organisation are adequate and are functioning effectively. Partner agencies will be required to provide quarterly updates to the NLSAB in relation to referrals received and outcomes. The NLSAB will 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.

The local authority will be required to provide updates to the NLSAB about PiPoT concerns relating to providers, colleges, and voluntary organisations not represented on the NLSAB.

5.2 Local Authority

Under section 6 of the Care Act 2014, the local authority has a duty to co-operate 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. The local authority safeguarding adults' team, overseen by the service manager can be contacted by partner organisations, for advice and guidance where required.

The Safeguarding Adults Team can be contacted by email safeguardingadultreferrals@northlincs.gov.uk or via telephone on 01724 297000.

The safeguarding lead 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.

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, or voluntary organisation. In these cases, the local authority 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 the local authority safeguarding adults' team will act as the lead organisation and coordinate a response, with the involvement and support of the relevant member organisations.

5.3 Agencies and voluntary organisations

All agencies, employers, student bodies and voluntary organisations, should have their own 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) 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 safeguard those adults.

All providers, voluntary agencies and other organisations who are not represented on the NLSAB will be required to provide quarterly updates to the local authority safeguarding adults team in relation to referrals received and outcomes. The local authority will the report this information to the NLSAB.

5.4 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 North Lincolnshire 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.

https://www.northlincscmars.co.uk/

5.5 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 GDPR; Article 4.

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.

Because the NLSAB is not an independent organisation registered with the Information Commissioner's Office (www.ico.org.uk) then the local authority will be the lead organisation (in terms of data controller) in the following instances:

- There is no clear lead.
- The information is not in the possession of any data controller.
- Two or more partner organisations are involved, and a co-ordinated response is required.

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 Social Work England, 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.

6. Required Action

The initial responsibility to share information and take action 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 proportionate to the circumstances and the person should be made aware of the decision to disclose the information.

Allegations against people who work with adults at risk must not be dealt with in isolation. Any corresponding action necessary to address the welfare of adults with care and support needs should be taken without delay and in a coordinated manner, to prevent the need for further safeguarding in the future.

7. 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 GDPR.

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.

If an allegation is made which concerns the actions of a professional, 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 Multi-Agency Safeguarding Adults policies and procedures, which gives guidance as to how S42 enquiries should be undertaken. It may also be appropriate for a PiPoT concern to run alongside an S42 enquiry.

APPENDIX 1: Data Protection Act 1998 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 paragraph’s as above.

What is personal data?

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

- from those data, or
- 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, also known as special category data, in Article 9 of the GDPR data means personal data consisting of information as to:

- The racial or ethnic origin of the data subject.
- His / her political opinions.
- His / her religious beliefs or other beliefs of a similar nature.
- Whether he / she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992).
- His / her physical or mental health condition.
- His / her sexual orientation.
- The commission or alleged commission by him/her of any offence, or
- 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.

Schedule 1 to the Data Protection Act 1998 and Article 5 of the GDPR lists the data protection principles in the following eight terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met

2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this act.
7. Appropriate technical and organisational measures shall be taken again unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

Section 1(4) of the Data Protection Act 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

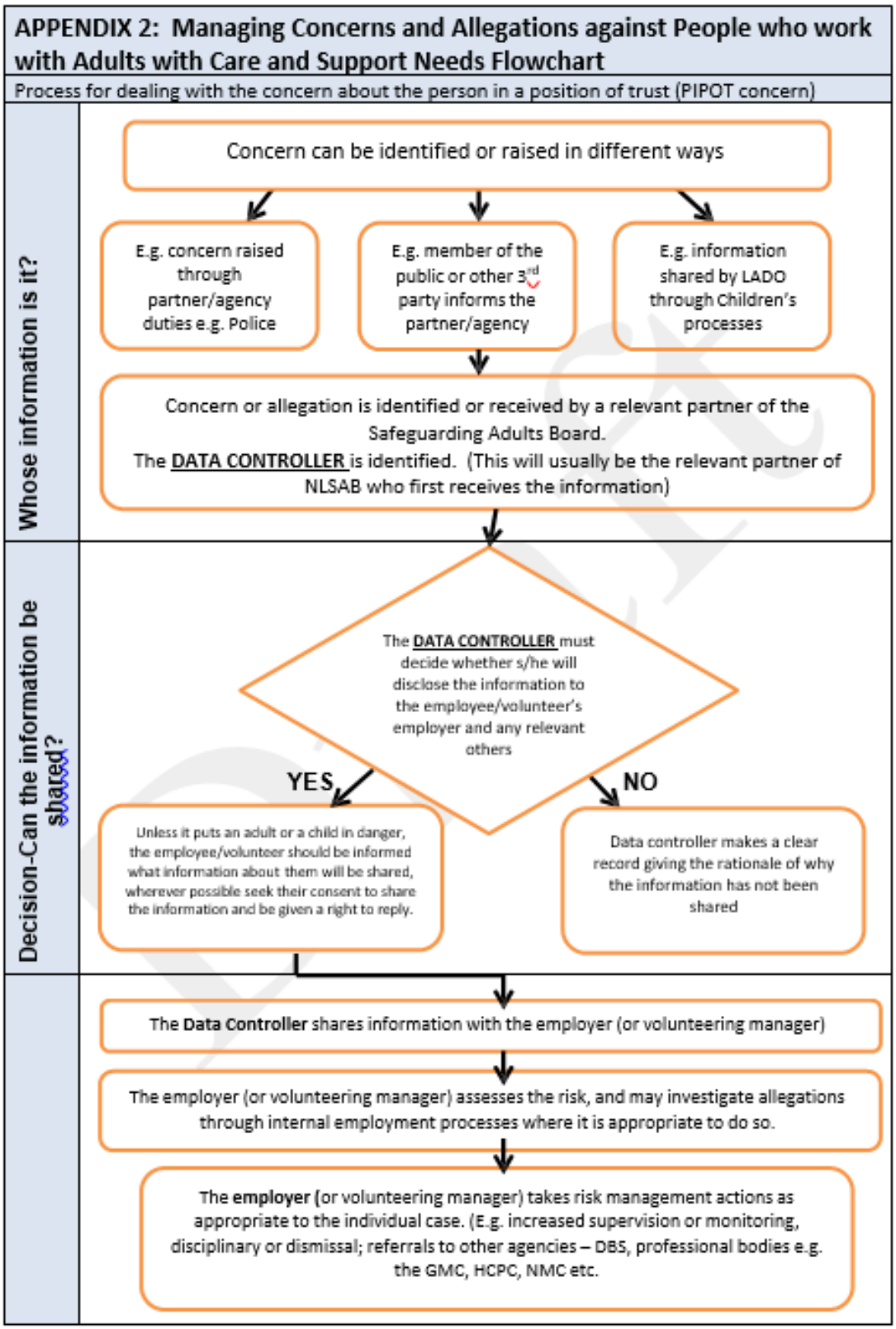
out certain aspects of the processing for it, overall responsibility remains with the organisation with the statutory responsibility to carry out the processing.

To determine whether you are a data controller you need to ascertain which organisation decides:

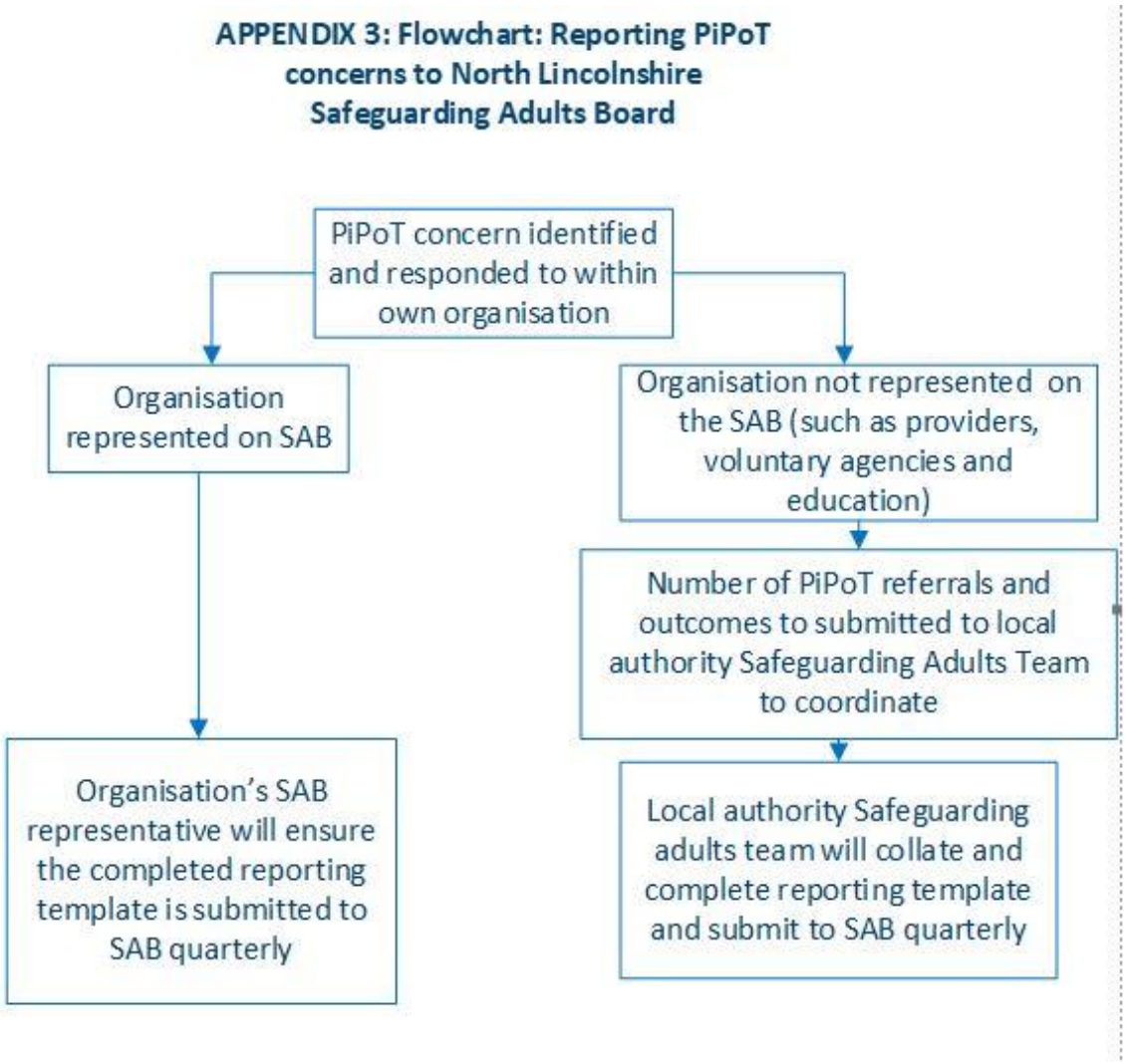
- To collect the personal data in the first place and the legal basis for doing so.
- Which items of personal data to collect, i.e., the content of the data.
- The purpose or purposes the data are to be used for.
- Which individuals to collect data about.
- Whether to disclose the data, and if so, who 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.



APPENDIX 3: Reporting PiPoT concerns to North Lincolnshire Safeguarding Adults Board



Safeguarding Adults Team

Email: safeguardingadultreferrals@northlincs.gov.uk

Telephone: 01724 297000

APPENDIX 4: Other legislation relevant to this policy

Other relevant legislation to this policy includes: The Data Protection Act 1998; General Data Protection Regulation 2018 (GDPR); Human Rights Act 1998 and employment legislation.

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)"

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 5: PiPoT reporting tool.

People in a Position of Trust (PiPoT) e-form reporting tool

Data collected (no identifiable information is requested).

- Organisation
- Name of person completing the form
- Reporting Period

All completed responses are collated via MS Forms.

- New referral this quarter
- Date of PiPoT
- Nature of the PiPoT
- Reference / identifying number.
- Current status of referral.
- Outcome.
- Actions required and status.
- Identified future learning.