Norfolk Safeguarding Adults Board

Information Sharing Agreement

Issue Number	FINAL
Document Author	
Document Owner	Norfolk Safeguarding Adults Board
Search Keywords	Information Sharing Agreement
For Use	By any agency or organisations to support safeguarding adults work
Document classification	Public
Date Approved	November 2025
Date Published on NSAB website	November 2025
Review Date	November 2028

Table of Contents

1. Purpose of information sharing 4
2. Information to be shared 5
3. Basis for information sharing – legislative context 6
4. Supply of information 8
5. Exchange of information 9
6. Terms of use of the information 10
7. Information and Data Quality Information 12
8. Data retention review and disposal 13
9. Access and security 13
10. General Operational Guidance/Process 14
11. Sharing with organisations who are not signatories to this agreement 15
12. Data Protection Impact Assessment 16
13. Rights of the data subject 16
14. Liability and indemnity 17
15. Management of the Agreement 17
16. Closure/termination of Agreement 18
17. Agreement 18

Appendix A The General Data Protection Regulation (UK GDPR) 19

Appendix B Caldicott Principles 23

This Information Sharing Agreement (ISA) is an agreement between all partner agencies working together under the remit of the Norfolk Safeguarding Adults Board (NSAB) to ensure the health, well-being, and safeguarding of adults in Norfolk who are in need of care and support. This agreement aims to facilitate the lawful and secure sharing of information between partner agencies and designated workers working to safeguard adults. The partners to this Agreement are also bound by the conditions set out in the Norfolk Overarching Information Sharing Protocol.

List of Partners in the Agreement

- Broadland District Council and South Norfolk Council
- Borough Council of King's Lynn & West Norfolk
- Breckland District Council
- Build Charity
- Care Quality Commission
- Department for Work and Pensions
- East Coast Community Healthcare C.I.C
- Great Yarmouth Borough Council
- James Paget University Hospitals NHS Foundation Trust
- Norfolk Care Association
- Norwich City Council
- Norfolk Community Health and Care NHS Trust
- Norfolk and Norwich University NHS Foundation Trust
- Norfolk and Suffolk NHS Foundation Trust
- Norfolk and Waveney Integrated Care Board
- Norfolk Constabulary
- Norfolk County Council
- Norfolk Fire and Rescue Service
- North Norfolk District Council
- National Probation Service, Norfolk
- The Queen Elizabeth Hospital King's Lynn NHS Foundation Trust
- Healthwatch Norfolk
- HMP Bure
- HMP Norwich
- HMP Wayland
- Office of the Police and Crime Commissioner for Norfolk
- University of East Anglia
- Voluntary Norfolk
- POhWER

1. Purpose of information sharing

1.1. Where there is specific information or concerns that an adult with care and support needs is being neglected, abused, or exploited or there is a risk of neglect or abuse, information will be shared between the partners (Care Act 2014 Section 42). It will be used to investigate the concerns and prevent the risk of neglect or abuse.

1.2. Only relevant, accurate and proportionate information will be disclosed to help appropriate partners to carry out safeguarding duties for which the data is necessary.

1.3. This ISA is underpinned by the following principles:

- The safety and well-being of adults with care and support needs is paramount in determining the need to share information.
- The partners have a responsibility to reduce risk of harm, abuse, or neglect to adults with care and support needs.
- Joint working is the most effective route to improving outcomes for adults with care and support needs.
- Information sharing is underpinned by the relevant partner agencies legislative framework, codes of professional conduct for managing confidential information and by policies for the assessment of risk and safeguarding adults with care and support needs.

1.4. NSAB continuously works towards ensuring the effective co-ordination of services to safeguard and promote the welfare of adults. It has a statutory duty under the Care Act 2014 to commission Safeguarding Adult Reviews when certain criteria is met (Section 44). Section 45 provides the statutory basis for the supply of information for the purpose of enabling or assisting the SAB to exercise its function. All information gathered throughout a review process will be treated as confidential and only shared when appropriate and in accordance with this agreement and its underpinning principles.

1.5. NSAB has a Quality Assurance framework (2022-25) which includes reference to multi-agency audits and partners who are signed up to this ISA are also signed up to the framework. Please refer to the Norfolk SAB Multi Agency Quality Assurance framework for further information (NSAB risk assessment and quality assurance | Norfolk Safeguarding Adults Board). Multi-agency case file audits assure the effectiveness of local systems and can identify both good practice and whether things could have been done differently. Data used for multi-agency audits will be anonymised for the purposes of a multi-agency audit.

2. Information to be shared

2.1. The Agreement concerns the following personal and/or sensitive information which needs to be shared for the purposes outlined in section 1:

- "Personal Data" which identifies the alleged victim(s) or alleged perpetrator(s) of abuse or neglect, e.g., name, date of birth, address.
- "Special Category Data" about the alleged victim(s) or alleged perpetrator(s) of abuse or neglect, e.g., gender, religion, ethnicity
- Reasons for concerns and details of the alleged concerns, e.g., type of abuse, location of abuse, levels of risk or urgency
- Information about the physical and or mental health of the alleged victim(s) or alleged perpetrator(s), e.g., mental capacity, communication needs
- Reports of any medical or social care assessments or examinations undertaken as part of the safeguarding adult's procedures, e.g., eligibility for community care, psychiatric assessment
- Personal Data which identifies professionals involved with the alleged victim(s) or alleged perpetrator(s)
- Personal Data which identifies other people who may be at risk, e.g., via employment, family, service.
- Historical information held in records about the alleged victim(s) or alleged perpetrator(s) that may be relevant to the current safeguarding concern or case review, e.g., previous safeguarding adults concern.
- Name and contact details of the person raising the concern (unless they have stated they wish to remain anonymous, and this anonymity would not have a detrimental impact upon the safeguarding adults process)
- Name of employer or organisation if the concern relates to a paid worker or volunteer of a service provider.
- The agreement also concerns aggregated data (e.g., statistics) which may be shared. In these situations, anonymised information should be used.
- Controller, Processor, Data Subject, Personal Data, Special Categories of Personal Data and Processing shall have the meanings given to them in the General Data Protection Regulation (UK GDPR) or the Data Protection Act 2018 (together "the Data Protection Legislation").
- Each partner subject to this agreement will retain exclusive control over the purpose for which the data is being processed. NSAB act on behalf of the partner organisations that make up the board, to collectively safeguard adults at risk, improve safeguarding practices and outcomes for individuals.
- NSAB is not a "controller" of data. In this context, as the individual(s) data subjects are not likely to have direct contact with the NSAB, the expectation would be that partners acknowledge on their own privacy notices that they may share information with the NSAB as they are the owners (data controllers) for the information.

3. Basis for information sharing – legislative context

3.1. Partners to this Agreement agree to act within and subject to existing legislative standards, any amendments thereto and any relevant legislation enacted or changes in the law hereafter.

3.2. The processing of information will satisfy:

- Article (6) (1) General Data Protection Regulation (UK GDPR) 2016 – see Appendix A
- Article 9 (2) General Data Protection Regulation – see Appendix A
- Human Rights Act 1998
- Care Act 2014
- Common law duty of care
- Common law duty of confidentiality
- Consent given by the adult.[1]
- Norfolk Safeguarding Adults procedures
- The Equalities Act 2010
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- The Mental Capacity Act 2005.

3.3 Partners must meet the requirements of Article 6 of the UK GDPR, for the processing of Personal Data by virtue of subsection 1(a), (d), (c) or (e):

a) the Data Subject has given explicit and informed consent to the processing of his or her personal data for one or more specific purposes.
b) processing is necessary for compliance with a legal obligation to which the Controller is subject); or
c) the processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

3.4 In the case of Special Categories of Personal Data, partners must also meet Article 9 condition by virtue of subsection 2 (a), (b), (c), (g) or (h):

a) the Data Subject has given their explicit consent to the processing of the personal data for one or more specified purposes, except where Union or Member State law provides otherwise.

[1] It may be preferrable wherever possible to obtain consent from an individual however this should not be relied upon if this is not a genuine choice for the data subject. Obtaining consent is not appropriate if partners to this agreement would still process the personal data for instance in the vital interest of the individual.

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.

c) processing is necessary to protect the vital interests of the data subject or another natural person in a case where the data subject is physically or legally incapable of giving consent

g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

h) for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 of Article 9.

3.5 In the case of criminal conviction and offence data, the processing meets the requirement in Article 10 of the UK GDPR for authorisation by the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1, 2 or 3 of Schedule 1. Article 10 restricts the processing of criminal offence data. Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carries out only under the control of official authority or when the processing is authorised by domestic law providing for appropriate safeguards for the rights and freedoms of data subjects

3.6 In respect of this Information Sharing Agreement Article 10 is met; the separate condition for processing criminal offence data is Article 6(e) Public Task, and Schedule 1, Part 2: Preventing or detecting unlawful acts; Safeguarding of children and of individuals at risk.

4. Supply of information

4.1 If a Safeguarding Adults Board (SAB) requests a person to supply information to it, or to some other person specified in the request, the person to whom the request is made must comply with the request if:

a) Conditions 1 and 2 (see below) are met; and

b) Condition 3 or 4 (see below) is met.

1) Condition 1 is that the request is made for the purpose of enabling or assisting the SAB to exercise its functions

2) Condition 2 is that the request is made to a person whose functions or activities the SAB considers to be such that the person is likely to have information relevant to the exercise of a function by the SAB

3) Condition 3 is that the information relates to:

a) The person to whom the request is made, or

b) A function or activity of that person, or

c) A person in respect of whom that person exercises a function or engages in an activity.

4) Condition 4 is that the information:

a) Is information requested by the SAB from a person to whom information was supplied in compliance with another request under this section; and

b) Is the same as, or is derived from, information so supplied.

5) Information may be used by the SAB, or other person to whom it is supplied under subsection (1) (see above), only for the purpose of enabling or assisting the SAB to exercise its functions.(Section 45 Care Act 2014)

4.2 Common law duty of care

The Police have a common law duty of care to protect the public and may share personal data where it is necessary to prevent harm.

4.3 Common law duty of confidentiality

This means that anyone proposing to disclose information not publicly available and obtained in circumstances giving rise to a duty of confidence, will need to establish whether there is an overriding justification for so doing. If not, it is necessary to obtain the informed consent of the person who supplied the information. This will need to be assessed on a case-by-case basis and legal advice should be sought in any case of doubt.

4.4 Consent

Partner organisations do not require the consent of the individual who is subject of the information in order to access or share their personal information if it is necessary in order for the Board to carry out its role, or to protect the vital interests of the individual concerned .However, it may be preferable, wherever possible to obtain consent from the individual, particularly where an individual may not expect their information to be passed on and where they also have a genuine choice about this. The data subject must be informed of their right to withdraw their consent.

Section 42 of the Care Act 2014 sets out the local authorities' duty to make safeguarding enquiries when the requirements are met. The involvement of the person in the safeguarding enquiry is not the same as requiring that persons consent to undertake the enquiry.

Where there is a public task that requires the sharing of information it is likely that the task rather than the individuals consent is a more appropriate lawful basis on which to share information This can be because it is overwhelmingly in the information subject's interests for this information to be disclosed, that an overriding public interest would justify disclosure of the information or that sharing is required in order to comply with a legal obligation

5. Exchange of information

5.1 Information will be exchanged when a partner organisation has a safeguarding concern about an adult with care and support needs, including where an organisation believes such an adult is being abused, exploited, or neglected or is at risk of neglect or abuse.

5.2 Any partner organisation that needs to refer an adult with care and support needs will contact Norfolk County Council Adult Care and verbally inform them when there are concerns.

5.3 When this happens, the organisation giving the information will always confirm the identity of the person receiving the information by making the telephone call via recognised contact details for Norfolk County Council.

5.4 An alternative to contacting Norfolk County Council by telephone is the online portal form - Contact our adult social care team - Norfolk County Council.

5.5 With regard to adults with care and support needs, consideration should be given to seeking consent to the sharing of information before disclosure to Norfolk County Council Adult Care.

5.6 In some circumstances information about a person **may be disclosed without their consent**. When overriding a person's wish for confidentiality, staff will be clear as to why this is being overridden and will document their reasons for doing so. Such reasons may include, but are not limited to the following:

- the adult with care and support needs lacks mental capacity to make an informed decision (MCA assessment documentation is required to support this)
- there is a risk of harm to the adult with care and support needs.
- there is potential risk of harm to others.
- an alleged abuser is an employee of any partner agency or voluntary worker with access to other adults with care and support needs.
- it is necessary for the detection and prevention of crimes (such disclosure to be necessary and proportionate to the crime being or alleged to have been committed)
- the condition for information sharing regarding the Domestic Violence Multi Agency Risk Assessment Conferences (MARAC) is met: 'to identify those victims who are of a high risk of serious harm, personal harm, or injury from domestic violence which is life threatening and or traumatic and from which recovery whether physical or physiological can be expected to be difficult or impossible.'

6. Terms of use of the information

6.1 The information that is shared will be used to assess the circumstances of the adult with care and support needs and the risk of neglect or abuse to that adult with care and support needs.

6.2 Information will be shared on a need-to-know basis only.

6.3 Any sharing of Personal Data must comply with the fair processing conditions outlined in the Data Protection Legislation. Consequently, information shall be:

- Obtained only for the purposes detailed in section 1
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- Accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
- Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed.
- Personal Data may be stored for longer periods in so far as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the Data Subject ('storage limitation')
- Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

6.4 For retention and destruction please see section 8 below.

6.5 The disclosure of the information must lead to a proportionate response when protecting a vulnerable person or persons.

6.6 Caldicott Principles will also apply to the processing of the information (see Appendix B):

- Where it is reasonably determined that further information is necessary to fulfil statutory duties and/or other requirements this Agreement will be reviewed in full or in part as appropriate
- Whenever possible data shared, should be anonymised, unless requested at personal level.
- Information on children, young people and adults will be shared with industry standard security.
- All parties will store Personal Data shared between partners on secure systems which can only be accessed by a restricted number of appropriate staff with appropriate security safeguards.

- All parties will use the data supplied for the purposes stated and will not pass such data to third party organisations outside the remit of specified partners in agreement without prior written consent unless required to do so by law.
- It is also prohibited under this agreement for sub-processors to be used without the prior consent of the Data Controller
- All parties will comply with their obligations under the Freedom of Information Act 2000 and may consult with another party if necessary if requests relate to information shared but will remain responsible for responding to the request.

7. Information and Data Quality Information

7.1 Each partner must recognise the importance of decision making based on information derived from robust systems and processes. All processes will be designed to support good quality data.

7.2 Information shared must be fit for purpose, which means that it must be adequate, relevant, and not contain excessive detail which is beyond that required for the agreed purpose.

7.3 Information discovered to be inaccurate, out-of-date, or inadequate for the purposes detailed in section 1 should be notified to the Data Controller – the original partner who has provided the information – who will be responsible for correcting the data and notifying all other recipients of the information who must make sure the correction is made.

7.4 Each partner will keep appropriate records of the sources of information to provide for this.

7.5 No secondary use or other use may be made unless the consent of the disclosing partner to that secondary use is sought and granted.

8. Data retention review and disposal

8.1 Each partner to this agreement will ensure that:

- They have in place and comply with their own policies and procedures governing the secure storage of all Personal Data within their manual and electronic storage systems, the retention of information held in manual and electronic systems, and the secure disposal of electronic and manually held information.
- Electronic copies of information are held on encrypted devices or servers and stored in UK EEA and should not be transferred to portable devices unless such devices are fully encrypted and their use is necessary for the provision of services under this Agreement.
- Information processed under this Agreement will only be retained for a minimum period as necessary in relation to the purpose for which it has been provided and then securely destroyed when that period comes to an end.
- Personal Data and Special Category Personal Data is securely removed from their systems and that printed documentation is securely destroyed at the end of its retention period.
- Electronic information will be securely destroyed by the physical destruction of the storage media or by the use of electronic shredding software that meets government standards or ISO 27001 to ensure permanent deletion.
- Hard copy information is destroyed by cross-cut shredding and secure recycling of the paper waste.
- All Personal Data is destroyed when no longer required for the purpose for which it was provided in accordance with their own secure destruction policy, unless the law requires that the Personal Data is retained.
- The information is reviewed every year to confirm that it remains accurate and relevant by the Norfolk Safeguarding Adults Board.

9. Access and security

9.1 Each Partner will make sure that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data.

9.2 Each partner shall make sure that measures are in place (including training) to do everything reasonable to:

- Make accidental compromise or damage unlikely during storage, handling, use, processing transmission or transport.
- Deter deliberate compromise or opportunist attack.
- Securely dispose of or destroy the data in a manner to make reconstruction unlikely.
- Promote confidentiality in order to avoid unauthorised access.
- Be ready and prepared to respond to any breach of security swiftly and effectively and the partner must ensure that any breaches are reported to the Data Controller within one working day (this is particularly important in light of the Data Protection Legislation as there will be significantly more liability if responsible for a breach)
- All breaches should be reported to the relevant Data Controller as quickly as possible as Data Controllers have specific responsibilities to report personal data breaches to the Information Commissioner without undue delay and where feasible not later than 72 hours.
- Maintain a record of Personal Data and processing activities regarding the data.

9.3 Signatory partners are expected to train their relevant staff and promote awareness of the major requirements of information sharing, including responsibilities in confidentiality and data protection.

9.4 Access to information subject to this agreement will only be given to those professionals who ‘need to know’ to effectively discharge their duties.

9.5 Information will only be communicated through the agreed channels.

10. General Operational Guidance/Process

10.1 All partners to this Agreement acknowledge and agree that the Personal Data held will be processed fairly and lawfully in accordance with the principles of the Data Protection Legislation and any supporting legislation.

10.2 The partners to this Agreement are members of the Norfolk Safeguarding Adults Board or support the wider partnership.

10.3 The Norfolk Safeguarding Adults Board Procedures contain specific guidance on recording, confidentiality and information sharing in section 6.

10.4 All complaints or breaches relative to this Agreement will be notified to the Norfolk Safeguarding Adults Board and the designated Data Protection Manager of the relevant partner organisation as soon as possible and within one working day in accordance with their own policy and procedures. The Norfolk Safeguarding Adults Board will be notified of any such complaint or breach, and the outcome, to make sure that appropriate action has been taken.

10.5 Disclosure of Personal Data without consent must be justifiable on statutory grounds or meet the criterion for claiming an exemption under the Data Protection Legislation.

10.6 Without such justification, both the partner and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the Data Protection Legislation or damages for a breach of the Human Rights Act 1998.

10.7 If the disclosure of Personal Data is in contravention of the requirements of the Data Protection Legislation, the partner who originally breached those requirements, either in requesting or disclosing information, shall indemnify the other partner against liability, cost or expense reasonably incurred.

10.8 The Norfolk Safeguarding Adults Board acknowledges that there will be occasions where workers/partners, with best intentions, may make mistakes regarding sharing information. Where this has been done in the mistaken belief that sharing information will safeguard an adult/child/young person, the Norfolk Safeguarding Adults Board expects the partner/employer to support their staff member and reinforce positive information sharing.

11. Sharing with organisations who are not signatories to this agreement

11.1 Any organisation who is not party to this overarching Agreement but who wishes to share information may do so, providing that there is an existing Information Sharing Agreement in place with the third party, that they agree to comply with the terms of this overarching protocol and have adequate technical and non-technical security arrangements in place.

12. Data Protection Impact Assessment

12.1 Under the Data Protection Legislation, a Data Protection Impact Assessment (DPIA), which is an assessment made to help identify and minimise the data protection risks of a project, is mandatory for certain listed types of processing. A DPIA must be carried out before personal data is processed when that processing is likely to result in a high risk to the rights and freedoms of individuals. The DPIA should take into account the nature, scope, context and purposes of the processing. Further information can be found on the ICO's website.

13. Rights of the data subject

13.1 Right to be forgotten/to withdraw consent

Under the UK GDPR, where a Data Subject has given their consent to the Processing of their Personal Data, he or she has the right to withdraw and revoke that consent at any time. Provided there is no other justification or legal obligation for continued processing, the Personal Data must then be erased.

13.2 However, where a Data Controller is relying on a legal obligation as the basis for Processing Personal Data, the Data Subject does not have the right to have their Personal Data erased, unless either of the following conditions apply:

- The Personal Data is no longer necessary or relevant in relation to the purpose for which it was original collected; or
- The Personal Data has been unlawfully processed, in breach of the Data Protection Legislation.

13.3 When deciding whether the right of erasure applies, the Data Controller must take into account the exceptions to the right and make a decision as to whether to comply with the request. Once a decision has been made, the Data Controller should confirm the decision in writing to the Data Subject and, if the right of erasure is engaged, ensure that the data is deleted within one month of the request. The Data Processors will comply with any instructions from the Data Controller to delete Personal Data in such circumstances.

13.4 Right to have data transferred

Under the UK GDPR an individual has the right to have their Personal Data transferred where all the below conditions are met in respect of the processing:

- The individual has provided their data to a controller.
- The processing is based on the individual's consent or for the performance of a contract; and
- The processing is carried out by automated means.

14. Liability and indemnity

14.1 Under the Data Protection Legislation, Data Subjects will be able to take action against both Data Controllers and Data Processors and potentially claim damages where they have suffered material or immaterial damage as a result of an infringement of obligations under the UK GDPR ("Compensation"). The Information Commissioner's Office can also fine a Processor or a Controller in relation to any breaches of the Data Protection Legislation.

14.2 In the event that the Data Controller or the Data Processor (for the purposes of this clause: "Party A") is ordered by a Court/Tribunal to pay Compensation to a Data Subject or is required to pay a fine by the Information Commissioner's Office, to the extent that such Compensation has arisen as a result of the act, negligence, omission or default of the other party ("Party B"), Party B shall indemnify Party A in respect of that element of the Compensation.

15. Management of the Agreement

15.1 The Agreement will be reviewed every three years and monitored by the Norfolk Safeguarding Adults Board Manager, unless new or revised legislation or national guidance necessitates an earlier review.

15.2 Complaints will be dealt with in a sensitive manner and recorded to enable the review and monitoring processes to be ethical. All complaints relevant to the sharing under this agreement will be dealt with under the Norfolk County Council Complaints Policy.

15.3 Requests for information under the Data Protection Legislation and Freedom of Information Act 2000 will be dealt with by the designated Data Protection Manager of the relevant partner agency in accordance with their own policy and procedures.

15.4 Where a request for information includes that information provided by a partner organisation, the originating organisation will be informed in accordance with normal protocols. However, each organisation is responsible for their compliance with the Freedom of Information Act 2000.

15.5 It is the responsibility of each partner signatory to the Agreement to ensure that they have the latest version of this Agreement.

15.6 All partners to the Agreement acknowledge and agree to comply with this Agreement.

16. Closure/termination of Agreement

16.1 This Agreement may be suspended by any partner for up to 30 days, in the event of any significant breach to negotiate appropriate remedial action.

16.2 Where negotiations do not successfully resolve the concerns of any partner, the Agreement may be terminated in writing with immediate effect.

17. Agreement

Agreement for……

We accept that this Information Sharing Agreement will provide a framework between the signatory organisations for the secure sharing of information within the

Norfolk Safeguarding Adults Board in a manner compliant with our statutory and workers responsibilities.

SIGNED…….

DATED……..

Appendix A The UK General Data Protection Regulation (UK GDPR)

The UK GDPR Principles

1. Personal data shall be:

a) Lawfulness, fairness and transparency

processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')b) Purpose limitation

collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')

c) Data minimisation

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

d) Accuracy

accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

e) Storage limitation

kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

f) Integrity and confidentiality (security)

processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against

accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

Specific Articles – 6 & 9

Article 6

CONDITIONS RELEVANT FOR PURPOSES OF PROCESSING OF ANY PERSONAL DATA

1) Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

c) processing is necessary for compliance with a legal obligation to which the controller is subject

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Article 9

CONDITIONS RELEVANT FOR PURPOSES OF PROCESSING OF SPECIAL CATEGORIES OF

DATA

1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2) Paragraph 1 shall not apply if one of the following applies:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject

c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects

e) processing relates to personal data which are manifestly made public by the data subject

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Appendix B Caldicott Principles

The Caldicott Report set out a number of general principles that health and social care organisations should use when reviewing its use of client information and these are set out below:

Principle 1: Justify the purpose(s) for using confidential information
Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary
Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information
Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis
Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities
Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with the law
Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.