

OFFICIAL



**NORFOLK**  
CONSTABULARY  
*Our Priority is You*



**SUFFOLK**  
CONSTABULARY  
*Taking pride in keeping Suffolk safe*

# INFORMATION SHARING AGREEMENT

**BETWEEN**

**NORFOLK CONSTABULARY,  
NORFOLK COUNTY COUNCIL,  
NORFOLK SCHOOLS,  
ACADEMIES, AND COLLEGES  
UNDER OPERATION  
ENCOMPASS**

## Summary Sheet

ISA Reference	<b>ISA/049 (ISA-003453-18)</b>
Purpose	<b>Operation Encompass</b> is a multi-agency approach to give early notification to schools, academies and colleges that a child or young person has been present, witnessed or been involved in a domestic abuse incident. Nominated Key Adults within local schools will receive information from Norfolk Constabulary to afford them the opportunity of assessing the needs of the child during the school day and, should it be deemed appropriate to do so, to provide early support.
Partners	Norfolk Constabulary Norfolk County Council Norfolk Schools, Academies and Colleges
Date of Agreement	June 2016 Amended: - September 2018 to comply with GDPR/ Data Protection Act 2018 November 2020 to reflect changes to delivery method
Review Date	November 2021
ISA Owner	Superintendent Safeguarding
ISA Author	Information Sharing Officer (updated by Data Protection Reform Team, September 2018)

## Consultation Record

Reviewer	Date of Approval
Data Protection Officer	
Head of Department owning the ISA	
Any Other Internal Stakeholders	
External Stakeholders	
Information Security Manager (where relevant)	
Information Asset Owner (s)	

## Version Control

Version No.	Date Amendments Made	Authorisation
Vr 1	21/09/2018	CR
Vr 2	25/09/2018	SC
Vr 3	04/12/2018	SC
Vr 4	06/12/2018	SC
Vr 5	13/12/2018	SC
Vr 6	18/12/2018	SC
Vr 7	14/02/2019	SC
Vr 8	21/02/2019	SC
Vr 9	12/03/2019	SC
Vr 10	11/12/2020	CF

## Contents

1. Introduction .....	4
2. Partners to the Agreement .....	4
3. Purpose .....	4
4. Lawful Basis.....	5
4.1 List of relevant statutory powers for Information Sharing.....	7
4.2 Framework legislation relevant to Information Sharing .....	7
4.3 Fair Processing Notice (FPN) .....	8
4.4 Legitimate Expectation .....	8
4.6 Freedom of Information Act .....	8
5. Data Protection Impact Assessment.....	9
6. Information Sharing Process/Procedures .....	9
8. Third Parties .....	12
9. Confidentiality and Vetting.....	13
10. Information Security .....	13
10.1 Information/Data Transfer .....	13
10.2 Security .....	13
10.3 Retention and Destruction .....	13
11. Operational requirements of this Agreement .....	14
11.1 Training and Awareness.....	14
11.2 Subject Access Request .....	14
11.3 Complaints, Security Incidents/Data Breaches/Losses.....	15
11.4 Data Quality.....	15
11.5 Ownership of the information and Indemnity.....	15
11.6 Commencement, Review and Audit .....	15
11.7 Termination.....	16
12. Signatures.....	17
APPENDIX A.....	18
APPENDIX B.....	21
APPENDIX C .....	22
APPENDIX D .....	23

## **1. Introduction**

For Parties to provide the most efficient and effective public services, it is often necessary to share appropriate and relevant personal information between organisations. Conversely, the concept of sharing public information can also raise public fear, anxiety and concerns over privacy invasion, which can lower trust and confidence in the police service and its partners and associated organisations.

The aim of this Information Sharing Agreement is to facilitate information sharing between Norfolk Constabulary, Norfolk County Council, Norfolk Schools, Academies and Colleges under Operation Encompass, to work together to improve public services within a framework of secure data handling measures and standards, which retain trust and confidence.

Operation Encompass is an initiative between Norfolk Police and local schools, academies and colleges to share domestic abuse (DA) information with nominated Key Adults where it is identified that a child was present, witnessed or was involved in such an incident. The sharing of this information will allow Key Adults to carry out an assessment of the needs of that child during the school day to determine what, if any, early intervention support is required to be put in place. The support that may be provided by the key adult can be overt or silent.

Throughout this Agreement, the term '*School*' will be used generically as representing all schools, academies and colleges in Norfolk who have signed up to the Agreement.

Parents, teachers, governors of schools and local councillors will be made aware of the implementation of Operation Encompass.

This Agreement is supported by the Operation Encompass Norfolk Joint Agency Protocol for Domestic Abuse – Notifications to Schools, Version 5.0.

This Agreement constitutes the entire agreement and understanding between the parties in respect of information passed under this Agreement and supersedes all previous agreements, understandings and undertakings in such respect.

## **2. Partners to the Agreement**

The Partners to this agreement are:

- 1) Norfolk Constabulary (the Constabulary)
- 2) Norfolk County Council (the Council)
- 3) The Schools signed up to Agreement

## **3. Purpose**

The purpose of this Agreement is to enable routine and effective information sharing between the Parties and to facilitate the lawful exchange of information in order to comply with the statutory duty on Chief Police Officers to safeguard children.

It sets out a multi-agency procedure to identify and provide appropriate early intervention support to a child who was present, witnessed or was involved in a DA incident.

The sharing of DA information between Norfolk Police and the Council (who will share with the Schools) will allow the school's nominated Key Adult to respond, if it is appropriate to do so, to the immediate needs of a child. The support that can be provided to address the emotional, health and well-being of the child can be overt or silent but is dependent upon the circumstances surrounding each incident.

The responsibility for providing support, or not as the case may be, will be down to the nominated key adult.

It is hoped, through the sharing of information between agencies and providing early Intervention support to a child as described above, Operation Encompass will reduce the impact of living with DA, which can result in anxiety, depression, aggression and post-traumatic stress disorder (PTSD).

Operation Encompass will enable DA to become an issue that can be discussed in schools and will not be seen as a 'taboo' subject. In other parts of the United Kingdom where Operation Encompass has already been implemented, parents are acknowledging the impact such abuse has on their children and have been prepared to talk to teachers about it.

The Agreement will be used to assist in ensuring that:

- Information is shared in a secure, confidential manner.
- Information is shared only on a 'need to know' basis.
- There are clear procedures to be followed with regard to information sharing.
- Information will only be used for the reason(s) it has been obtained.

#### **4. Lawful Basis**

This Agreement has been prepared with the obligations of the statutory guidance, the "Management of Police Information" (MoPI) in mind. The College of Policing Authorised Professional Practice (APP) Information Management, "MoPI sharing" provides standards that must be applied by the Chief Constables of Norfolk and Suffolk Constabularies when sharing information with external agencies. This Information Sharing Agreement (ISA) is compliant with such standards.

It is the responsibility of each Party to ensure that any processing of personal information owned by that Party is carried out in accordance with the requirements and principles of relevant legislation, including the General Data Protection Regulation (GDPR), the Data Protection 2018, the common law duty of confidentiality and the Human Rights Act 1998.

Personal data shall be processed fairly and lawfully, in a transparent manner, and in particular, shall not be processed unless at least one of the lawful bases for processing exists under Article 6 of the GDPR.

For the purposes of this Agreement the relevant condition is Article 6(e) necessary for the performance of a task carried out in the public interest. The public tasks are:

- Section 10 of the Children Act 2004 (the CA) - the duty to promote co-operation between the Parties with a view to improving the well-being of children in Norfolk and;
- Section 11(2) of the CA – the duty to ensure that the Parties' functions are discharged having regard to the need to safeguard and promote the welfare of children.

## OFFICIAL

Special category personal data (SCPD) (*i.e. racial/ethnic origin, political opinion, religious beliefs, trade union membership, genetics, biometrics, physical/mental health, sexual life or sexual orientation*) shall be processed fairly and lawfully, in a transparent manner, and in particular, shall not be processed unless at least one of the lawful bases for processing exists under Article 6 of the GDPR and a condition under Article 9 is met.

For the purposes of this Agreement the relevant condition under Article 9 is Article 9(2)(g) – necessary for reasons of substantial public interest and, as required under the Data Protection Act 2018 (the DPA) as follows:

For the Council:

- For exercise of a function conferred by enactment and necessary for reasons of substantial public interest under Schedule 1, Part 2, Paragraph 6 of the DPA. The relevant statute is Section 10 and Section 11(2) of the CA

For the Constabulary:

- For the purposes of a function conferred on a person by an enactment or rule of law under Schedule 1, Part 2, Paragraph 6 of the DPA.
- Necessary for the purposes of protecting the physical, mental or emotional wellbeing of an individual under the age of 18 under Schedule 1, Part 2, Paragraph 18 of the DPA.

For Schools:

- For exercise of a function conferred by enactment and necessary for reasons of substantial public interest under Schedule 1, Part 2, Paragraph 6 of the DPA. The relevant statute is Section 10 and Section 11(2) of the CA, Section 175 Education Act 2002

Personal data relating to criminal convictions and offences or related security measures shall be processed fairly and lawfully, in a transparent manner, and in particular, shall not be processed unless at least one of the lawful bases for processing exists under Article 6 and a separate condition for processing special category data under Article 9 is met, and it shall be carried out only under the control of official authority.

For the Council:

- The processing meets the requirement in Article 10 of the GDPR for authorisation by the law of the United Kingdom as it is in accordance with section 10(5) of the DPA in that the processing meets the condition in Schedule 1, Part 2, Paragraph 6(1) and 6(2) of DPA i.e. necessary for exercise of a function conferred by an enactment or rule of law as set out in section 10 and 11 of the CA and necessary for reasons of substantial public interest

For the Constabulary:

- The processing meets the requirement of Article 10 of the GDPR for authorisation by law of the United Kingdom as it is in accordance with Section 10(5) of the DPA in that the processing meets the condition in Schedule 1, Part 2, Paragraph 18 and 6 of the DPA i.e. Safeguarding children at risk and for the purposes of a function conferred on a person by an enactment or rule of law

For Schools:

- The processing meets the requirement in Article 10 of the GDPR for authorisation by the law of the United Kingdom as it is in accordance with section 10(5) of the DPA in that the processing meets the condition in Schedule 1, Part 2, Paragraph 6(1) and

6(2) of DPA i.e. necessary for exercise of a function conferred by an enactment or rule of law as set out in section 10 and 11 of the CA, Section 175 of the Education Act and is necessary for reasons of substantial public interest.

The sharing of information under this Agreement will be compliant with the European Convention of Human Rights and the Human Rights Act 1998, in particular Article 8 which states that: *'Everyone has the right to respect for his private and family life, his home and his correspondence'*.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

This Agreement takes into account the Common Law duty of confidentiality which applies where information has a necessary quality of confidence or where information is imparted in circumstances giving rise to an obligation of confidence that is either explicit or implied. Where the duty applies, disclosure will be justified through consent, legal duty, and the public interest or for the safeguarding of one or more people.

The following highlights relevant legislation and how information sharing for the purpose of Operation Encompass is viewed in respect of that legislation.

#### **4.1 List of relevant statutory powers for Information Sharing**

This agreement takes into account the following legislation and/or common law:

- Sections 10 and 11 (2) of the Children Act 2004;
- Common Law
- Education Act 2002

See <http://www.legislation.gov.uk/> for relevant details of each statutory power.

#### **4.2 Framework legislation relevant to Information Sharing**

This agreement takes into account the following framework legislation and/or common law:

- The General Data Protection Regulation (GDPR) and the Data Protection Act 2018
- The Human Rights Act 1998
- Common Law Duty of Confidence
- The Freedom of Information Act 2000
- Sub Judice – Contempt of Court Act 1981

See <http://www.legislation.gov.uk/> for relevant details of each framework legislation.

It is recognised that different Parties will need to rely on differing legal basis for information sharing depending on the legal status of that Party.

It is also acknowledged that it is the responsibility of each Party to decide on whether and what information will be shared. However, each Party agrees to the overriding principle that

information will be shared for the purpose of Operation Encompass where it is necessary, lawful and proportionate to do so.

Each Party will treat all police data ethically, with integrity, fairness, honesty, respect, accountability, objectivity and transparently in line with the Police Code of Ethics and/ or their organisations policies and procedures.

See <http://www.college.police.uk/What-we-do/Ethics/Ethics-home/Pages/Code-of-Ethics.aspx> for full details of the Police Code of Ethics.

### **4.3 Fair Processing Notice (FPN)**

To meet the GDPR transparency requirements, individuals should be provided with privacy information, as required under Article 13 and 14 of the GDPR including the purpose for processing their personal data, the retention periods for that personal data, and details relating to who the information will be shared with.

Where consent is not sought from the data subject for the processing of their personal data, it should be possible for the data subject to make reference to a Fair Processing Notice owned by the organisation/ agency processing their data. For example, Norfolk Constabulary can rely on the Force Information Charter on their website in order to meet the GDPR transparency requirements. The Schools in this Agreement will ensure parents receive a Fair Processing Notice.

### **4.4 Legitimate Expectation**

The sharing of information by the Constabulary must fulfil a policing purpose. A policing purpose is defined under the Management of Police Information (MoPI) Code of Practice as:

- Protecting life and property;
- Preserving order;
- Preventing the commissioning of offences;
- Bringing offenders to justice; and
- Any duty or responsibility of the police arising from common or statute law.

It can be reasonably assumed that the persons from whom information is obtained will legitimately expect that the Constabulary will share it appropriately with any person or party that will assist in fulfilling the policing purposes mentioned above. Reference to the Force Information Charter would also provide them will full details.

### **4.6 Freedom of Information Act**

If a Party receives a request for information under the Freedom of Information Act 2000 ("FOIA") and the Environmental Information Regulations 2004 ("EIR") all parties shall assist and co-operate with the other to enable the other party to comply with its obligations under FOIA and the EIR. This is in line with the requirements laid out in the Lord Chancellor's Code of Practice issued under section 45 of FOIA.

This Code of Practice contains provisions relating to consultation with others who are likely to be affected by the disclosure (or non-disclosure) of the information requested. The code also



relates to the process by which one authority may also transfer all or part of a request to another authority if it relates to information they do not hold.

Where a party receives a request for Information in relation to information which it received from another Partner, it shall: -

(a) contact the other party within 2 working days of receiving a request for Information;

(b) the originating authority will provide all necessary assistance as reasonably requested by the party to enable the other party to respond to a request for Information within the time for compliance set out in Section 10 of the FOIA or Regulation 5 of the Environmental Information Regulations.

In the interests of transparency, and to assist in meeting the fairness principle, this Agreement and the arrangements it details will be suitable for disclosure for the purposes of the Freedom of Information Act 2000 and so will be published within the Parties' Publication Schemes.

## **5. Data Protection Impact Assessment**

A Data Protection Impact Assessment (DPIA) is a process to identify and minimise data protection risks of a project. Where processing is likely to result in a high risk to individuals a DPIA must be undertaken (a definition of high risk is contained within the DPIA Guide which is available from the Information Management department).

The Parties have completed a DPIA screening checklist in order for an assessment to be made as to whether a DPIA is required in respect of this Agreement.

This Agreement describes the formalisation of a pre-existing and lawful process and presents no additional privacy concerns. Each organisation will determine if a DPIA is required for the purposes of sharing.

## **6. Information Sharing Process/Procedures**

It is recognised that the handling of such confidential, sensitive information needs to be dealt with in a way that is proportionate and appropriate to the needs of the child or young person. To address this, Key Adults will be identified in each school (a person with child safeguarding training). Where DA information is shared with Key Adults, the key adult will ensure that any records they have made will then be stored and secured in a similar manner to child safeguarding files.

The key adult will be the person available each day to receive the details of the DA incident and assess the type of support needed for the child. Norfolk Constabulary will hold a database of all Key Adults in the Norfolk area.

The process for sharing information is set out below and in **Appendix C** and within the Operation Encompass Norfolk Joint Agency Protocol.

The Constabulary will securely email the Operation Encompass mailbox, a spreadsheet of the following information every morning:

## OFFICIAL

- the fact that the police were called out in the last 24 hours to a DA incident and a child was present, witnessed or was involved in it (incidents occurring during the weekend, including Friday evening, will also be disclosed on the following Monday);
- the police reference number;
- the time and date of the event;
- circumstances surrounding the incident; this may include data relating to convictions or offences i.e. breach of bail conditions
- the names and dates of birth of any child from that school who was present, witnessed or was involved in the DA incident when it took place; and
- any other relevant safeguarding information that may assist the school in providing early intervention support to the child being referred.

The Council will share with the (relevant child's) Schools key adult, information relating to the DA incident that is considered relevant and proportionate to enable the school to take appropriate action.

In addition, the council will hold:

- A database of trained Key Adults. (They must also ensure that there is a sufficiently trained deputy to receive the information in their absence and any changes to the database must be reported to the single point of contact (SPOC) as soon as practicable)
- A contact email address for the key adult; and
- A contact telephone number for the key adult to be contacted on.

The School will use the information as set out and will not onwardly disclose the information received from the Council. A record will be securely held in the child's safeguarding file.

### 7. Roles and Responsibilities under this Agreement

The people who will have access to the information under this Agreement are: Norfolk Constabulary (ICO Registration number Z4894872)  
DI Christopher McGiven– MASH Domestic Abuse Safeguarding Team

Norfolk County Council Children's Services (ICO Registration number Z534327X)  
CADS Education Representative – Learning & Inclusion Service, Norfolk County Council  
Claire Farrelly, Safeguarding Adviser - Learning & Inclusion Service, Norfolk County Council  
Norfolk Schools – Key Adults – Register maintained by Norfolk County Council

The Constabulary and the Council's Children's Services must identify a single point of contact ("SPOC") who will be responsible for the development of this Agreement on behalf of the relevant business area and the first port of call for any questions about this agreement. The "SPOC" will also be responsible for any reviews or amendments to the Agreement. The "SPOC" for each partner should also be notified of any breach or dispute and will be responsible for obtaining authorisation to disclose any information to a third party.

SPOC's should maintain regular contact with each other and ensure that appropriate audit trails of sharing are retained and made available when required. Any changes in SPOC will

be notified in writing as soon as practicable and in any event within 5 working days after such a change has occurred.

The SPOCs are:

Name: T/DCI Pippa Hinds  
Position: Safeguarding T/DCI

Norfolk County Council Children's Services  
Name: Claire Farrelly  
Position: Safeguarding Adviser– Education Quality Assurance, Intervention & Regulation Service

Schools – Individual school's Key Adults

Only appropriate and properly authorised persons will have access to the information specified in this Agreement. If in doubt, a person intending to share or access information should contact their SPOC or Data Protection /Information Management Team.

All Parties must be fully aware of their obligations under the GDPR and DPA 2018 and must have the appropriate training, policies and procedures in place to ensure compliance.

It will be the responsibility of all partners to ensure that:

- Realistic expectations prevail from the outset
- Ethical standards are maintained
- A mechanism exists by which the flow of information can be controlled
- A mechanism exists by which the integrity of the data is upheld
- Appropriate training with regard to both this agreement and the GDPR and DPA 2018 in general is given to all relevant staff
- Adequate arrangements exist to audit adherence to the Agreement
- The sharing is covered under each party's privacy information notice

The Parties are aware that the deliberate or reckless disclosure of personal data (obtained under this Agreement) to other organisations or persons may amount to a criminal offence under the DPA.

### **The Constabulary's role**

The Constabulary will collate and prepare a spreadsheet of all domestic incidents where a child was present. This will be emailed to Children's Services staff within the Education Quality Assurance, Intervention & Regulation Service (EQAIRS).

### **The Council's Education Quality Assurance, Intervention & Regulation Service (EQAIRS) Role:**

The Council's **EQAIRS** will

- place the information on the Liquid Logic/PSS/Core+ case management system and
- identify the relevant School(s)
- e-mail these Schools using the AnyComms+ before 9am to notify them of the incident and provide sufficient information to the Schools so that the Schools are able to provide emotional support for children involved
- keep an accurate record of all notifications made
- keep an accurate record of named Key Adults for each education provider
- maintain the register of schools who are partners in the Agreement

## **The Council's Overarching Role**

The Council will

- provide a briefing session for all designated Key Adults nominated by their school, prior to the school receiving notifications.
- Ensure the briefing session is relevant and informative.
- ensure briefing sessions are regular and spread through the localities to maximise courage.
- regularly review Operation Encompass

## **The School's role:**

The Schools will

- ensure there is a Key Adult and deputy within the school and that they have attended the appropriate briefing prior to receiving notifications. This must be a trained DSL with responsibility for safeguarding.
- ensure the Key Adult signs the Operation Encompass Agreement (See Appendix D) and returns it to designated officer.
- ensure the Key Adult is available to receive the notification from Children's Services staff each morning
- ensure they keep an accurate record of each notification and store it utilising the current process used to store child protection paperwork within the school.
- provide silent or overt support to child, following a notification.
- provide EQAIRS with an up-to-date list of the Key Adults within their school, contact numbers and email addresses.

## **8. Third Parties**

Information shared under this Agreement must not be disclosed to any third party without the written consent of the Party that provided the information. It must be stored securely and deleted when it is no longer required for the purpose for which it was provided.

If any information shared under this agreement is intended for disclosure to any third party outside this agreement the partner making the intended disclosure will consult the originating partner prior to the disclosure being made.

Disclosure of personal data must be relevant. Only the minimum amount of information that needs to be shared to achieve the purpose for sharing it shall be supplied. Where a report is received regarding a child who resides in Norfolk but attends an out of county school then this information will not be shared as they are not covered by this protocol.

The identity of the originator must be recorded against the relevant data. No secondary use or other use may be made of the information unless the consent of the disclosing party to that secondary use is sought and granted in writing.

Disclosure must be compatible with the second data protection principle:

'Personal data shall be 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 purpose ('purpose limitation'). (Article 5 (1(b)) General Data Protection Regulation)

## **9. Confidentiality and Vetting**

The information shared under this Agreement is classified under the Government Security Classification Scheme as OFFICIAL-SENSITIVE. Under the GSC, handling caveats/ conditions may also be applied in addition to the protective marking; these will be clear and self-evident as to their meaning or requirements.

Vetting is not mandatory to view this grade of information; however, staff working in the Council and Schools will either be vetted to NPPV level 2 or have an 'Enhanced' DBS check. What is required at this level of access is a strict 'need-to-know' the information, which all staff viewing shared information must have.

## **10. Information Security**

### **10.1 Information/Data Transfer**

Information will be transferred electronically between the Parties using secure e-mail networks only, such as pnn or cjsm or by recorded delivery, telephone, and verbally at meetings or in person.

The Parties will take into consideration the requirements of the GDPR including Articles 44-49 in relation to international transfer.

- 44-General principle for transfers
- 45-Adequate levels of protection
- 46-Transfers subject to appropriate safeguards
- 47-Binding corporate rules
- 48-Transfers or disclosures not authorised by Union Law
- 49-Derogations for specific situations

Should any Parties wish to transfer information to a third country or to an International organisation they must liaise with their Data Protection Officer for further advice.

### **10.2 Security**

All agencies that are provided information under this Agreement are required to conform to the following Norfolk & Suffolk Constabularies Information Security Policy Statement – **Appendix A**, for the purpose of ensuring that a suitable standard for Information Security is maintained.

### **10.3 Retention and Destruction**

The information will be retained by Parties under Operation Encompass in line with existing and established business processes, guidelines and legislation. The Constabulary will retain information in line with MOPI whilst the Council and the Schools will retain information in line with their organisation's retention period. All hard copies will then be destroyed by use of a cross shredder. All information on computer systems will be securely deleted.

## **11. Operational requirements of this Agreement**

### **11.1 Training and Awareness**

All Parties will ensure that all individuals likely to come in contact with the data shared under this agreement are trained in the terms of this agreement, their own responsibilities and their obligations under the GDPR and the DPA.

### **11.2 Subject Access Request**

All Parties will comply with the requirements of the **GDPR** including Articles 12-22 in relation to subject rights.

- 12 – Exercise of the rights of the data subject
- 13 – Information to be provided where personal data are collected from the data subject
- 14 – Information to be provided where personal data have not been obtained from the data subject
- 15 – Right of access by the data subject
- 16 – Right to rectification
- 17 – Right to erasure ('right to be forgotten')
- 18 – Right to restriction of processing
- 19 – Notification obligation regarding rectification or erasure of personal data or restriction of processing
- 20 – Right to data portability
- 21 – Right to object
- 22 – Automated individual decision-making, including profiling

Any Party receiving a written or verbal request for subject access to personal information under Article 15 of the GDPR relating to information shared under this Agreement must direct the request to their Data Protection Officer who will consult with the other Parties prior to the release of any information provided by those Parties. In order to facilitate this, information should be clearly labelled to identify the source Party.

If a Party receives a subject access request and personal data is identified as originating from another agency, it will be the responsibility of the receiving agency to contact the data provider within 2 working days (of becoming aware that Operation Encompass forms part of the request) to consult on the application of potential exemptions under the provisions of the Data Protection Act 2018.

If a Party receives a request from an individual to exercise a right to erasure, rectification, restrict processing, or objection to processing in respect of information shared under this Agreement, it will be the responsibility of the receiving party to contact the other Party within 2 working days to inform them of the action taken. It will also be the responsibility of the receiving party to inform the individuals about the recipient(s) of the relevant personal data.

### **11.3 Complaints, Security Incidents/Data Breaches/Losses**

Any complaints received by the Parties from individuals about the process or procedural issues relating to this Agreement, or regarding information held by any of the parties to this Agreement, will be referred to the Data Protection Officer for the relevant Party for investigation. Where such complaints relate to alleged inaccurate information the Parties will liaise with the Data Protection Officer of the party involved and the appropriate course of action will be taken.

Any potential data loss or breach of Data Protection legislation, including information shared under this agreement being disclosed outside of this agreement, should immediately be brought to the attention of the relevant Parties Business Lead(s), Data Protection Officer, and their counterpart(s) within the other relevant Party. Depending on the urgency, notification of the breach can be made initially verbally and then sent via email. It will be the responsibility of the respective controller to report the incident immediately and to follow their security incident reporting procedures. Should a breach be reported to the Constabulary's Business Lead(s), they shall, without delay, complete and submit an Information Security Incident Form to Information Security who shall deal with the breach in line with the policy.

### **11.4 Data Quality**

It is the responsibility of all Parties to ensure that the information is of sufficient quality for its intended purpose, bearing in mind accuracy, validity, reliability, timeliness, relevance and completeness. All information should be checked in respect of quality prior to being shared.

Information discovered to be inaccurate or inadequate for the purpose will be notified to the data owner who will be responsible for correcting the data and notifying all other recipients of the data who must ensure that the correction is made.

All Parties must have processes in place to monitor and check the quality of information.

### **11.5 Ownership of the information and Indemnity**

The Chief Executive/Officer of the Party holding the personally identifiable information will be the Controller. The Chief Executive/Officer of the Party receiving the information will become the Controller on receipt and will be responsible for ensuring that the information is held and used securely in accordance with Data Protection legislation, other relevant legislation, this Agreement and will accept total liability for a breach of this Agreement should any legal proceedings be served in relation to the breach.

There is no requirement for an indemnity in relation to this ISA as the responsibility of Data Controller passes to the receiving party.

The Parties shall not assign, sub-contract or transfer its rights or obligations under this Agreement in whole or part to any third party without prior written consent of the other parties.

### **11.6 Commencement, Review and Audit**

This Agreement replaces the previous Information Sharing Agreement between the Parties, which commenced from the start of the Autumn Term 2016 and amended in 2018.

## OFFICIAL

This Agreement will be reviewed on an annual basis. Interim reviews of this Agreement may, however, be carried out at the specific request of any of the Parties.

Each Party will ensure they keep an audit trail of all information shared and received in relation to the purpose and processes of this Agreement.

Each Party will provide the other Party on reasonable request with evidence that all aspects of this Agreement are being complied with.

The Parties will allow the other Party to carry out an audit to ensure each Party is in compliance with this Agreement.

The Parties will complete the Norfolk & Suffolk Constabulary Annual Audit Declaration - **Appendix B** on request. The SPOC for Norfolk Constabulary will be responsible for ensuring that the Parties complete the Annual Audit Declaration.

The Parties will report all issues, complaints or queries about the operation of this Agreement at each of its reviews and the outcomes recorded in writing.

### **11.7 Termination**

This Agreement may be terminated at any time upon receipt of a written request from any of the Parties and with the agreement of the other Parties.



## 12. Signatures

**Organisations signatures: I confirm I have read and understood this agreement and am duly authorised to sign this agreement. I hereby agree to the terms and conditions imposed therein.**

**Name of Organisation:** Norfolk Constabulary

Name: Paul Sanford

Position: Deputy Chief Constable

Signature:



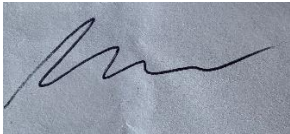
Date: 04/12/2020

**Name of Organisation:** Norfolk County Council

Name: Marcus Needham

Position: Head of Quality Performance & Systems, Children's Services

Signature:



Date: 04/12/220

Contact Telephone Number: 01603 217726

**Further details to be added as the school joins the Agreement.**

## APPENDIX A

### **Constabulary Information Security Policy Statement**

All Chief Constables are committed to compliance with the Community Security Policy, and they and Partner Organisations are expected to ensure that all data and information is handled in line with the HMG Security Policy Framework, specifically meeting the following Mandatory Requirement:

Departments and Agencies must have an information security policy setting out how they and any delivery partners and suppliers will protect any information assets they hold, store or process (including electronic and paper formats and online services) to prevent unauthorised access, disclosure or loss. The policies and procedures must be regularly reviewed to ensure currency.'

#### Scope

These Information Security Requirements and Objectives apply to the following:

- Roles & Responsibilities  
All persons or parties conducting work for either Signatory regardless of any form of employment, including contractors providing services, agency workers and trainees on vocational or work experience.
- Data & Information
  - Whether stored, copied, duplicated or transmitted, all 'soft' (electronic, digital and virtual) data, information and communications on servers, networks, connectivity, ICT kit such as PCs, workstations, laptops, and authorised multimedia devices including USBs, mobile phones, tapes and CDs.
  - Also 'hard' information printed or written on paper or other medium such as whiteboards and flipcharts, and transmitted by any method whatsoever, such as fax or scanner.
  - Additional safeguards should be considered, specified and documented according to the sensitivity and classification of the data, information, and/or circumstances of the Agreement, for example observing operational security, such as precautions against eavesdropping.
- Data: The Data Protection Act & Information Commissioner's Office
  - Where Signatories process personal data defined by the Act, they agree to apply security measures, commensurate with principle 6 of the Data Protection Act 2018: "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)
  - These Information Security Requirements and Objectives should evidence this principle.

#### Information Security Requirements & Objectives

To that end, Signatories to this agreement should ensure, document and be able to evidence, that they have in place common technical and organisational security arrangements,

evidencing the following appropriate, proportionate and reasonable Information Security Requirements and Objectives:

- Information Security risk assessments to establish, evaluate and accept risks, and put in place appropriate controls to manage them.
- Information Security Policies, Guidelines, Processes, Controls and Practices in place to protect, and ensure the confidentiality, integrity and availability of data and information and systems under their control.
- An Information Security Review process at planned intervals, so that should significant changes occur this will ensure their continued suitability, adequacy, and effectiveness; i.e. for technological, legal, contractual and regulatory requirements and organisational changes.

Specifically, they should address the Information Security Requirements and Objectives below.

- **Information Security Policy** - A documented Information Security Policy should provide governance, management direction and support for information security according to relevant business and organisational requirements, contractual obligations, laws, statutes, regulations and best practices.
- **Organisation of Information Security** - Internal Organisation & External Parties to manage information security within the organisation and maintain the security of information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.
- **Asset Management** - Responsibility for Assets & Information Classification to achieve and maintain appropriate protection of organisational assets, and ensure information receives an appropriate level of protection.
- **Human Resources Security** - Prior to, During & After Employment. Training & Awareness to ensure that employees, contractors, third parties, and other users understand their responsibilities, and are suitable for the roles they are considered; reducing the risk of theft, fraud or misuse of facilities; and are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support security policy in their normal work, reducing the risk of error; and to ensure that all users exit or change employment in an orderly manner. Information security programmes should be available and imparted to all relevant users.
- **Physical & Environmental Security** - Secure areas & Equipment Security to prevent unauthorised physical access, damage and interference to the organisation's premises and information; and prevent loss, damage, theft or compromise of assets and interruption to the organisation's activities.
- **Communications & Operations Management** - Operational Procedures, Responsibilities & Third-Party Service Delivery Management to ensure the correct and secure operation of information processing facilities; and implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements;
- **System Planning** - Acceptance & Protection against malicious & mobile code to minimise the risk of systems failures; and protect the integrity of software and information;
- **Back-up & Network Security Management** - To maintain the integrity and availability of information and information processing facilities and ensure the protection of information in networks and the protection of the supporting infrastructure.

- **Media Handling** - Exchange of Information & Monitoring to prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities; maintain the security of information and software exchange internally and with any external entity; and detect unauthorised information processing activities.
- **Electronic Commerce Services** - To ensure their security, and secure use.
- **Access Control**
  - Business Requirement for Access Control & User Access Management to control access to information, ensuring authorised user access, preventing unauthorised access to information systems.
  - User Responsibilities & Network Access Control to prevent unauthorised access, compromise, theft of information and information processing facilities; and access to networked services.
  - Operating System, Access, Application, & Information Access Control to prevent unauthorised access to operating systems; and information held in application systems.
  - Mobile Computing & Teleworking to ensure information security when using mobile computing and teleworking facilities.
- **Information Systems Acquisition, Development & Maintenance**
  - Security Requirements of Information Systems & Correct Processing in Applications to ensure that security is an integral part of information systems, and prevent errors, loss, unauthorised modification or misuse of information in applications.
  - Cryptographic Controls & Security of System Files to protect the confidentiality, authenticity or integrity of information by cryptographic means, and ensure the security of system files.
  - Security in Development, Support Processes & Technical Vulnerability Management to maintain the security of application system software and information, and reduce risks resulting from exploitation of published technical vulnerabilities.
- **Information Security Incident & Breach Management** - To report information security threats, events and weaknesses ensuring those associated with information systems are communicated to allow timely corrective action; and manage incidents and improvements, ensuring a consistent and effective approach is applied to information security incidents.
- **Business Continuity Management** - To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
- **Compliance with Legal Requirements** - To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements, and that they are met wherever applicable; and to ensure compliance of systems with organisational security policies and standards, and to maximize the effectiveness of and to minimise interference to/from the information systems audit process.



## ANNUAL AUDIT DECLARATION FOR THE OPERATION ENCOMPASS INFORMATION SHARING AGREEMENT

“I confirm that I have sample checked a number of requests for police information to ensure all police information received has only been used/processed in line with the Operation Encompass Information Sharing Agreement. Any exceptions have been reported to Norfolk & Suffolk Constabularies.”

“Additionally, I can confirm that all procedures and processes stated in the Operation Encompass Information Sharing Agreement are currently in place.”

Period .....*Put in relevant dates*

ORGANISATION:

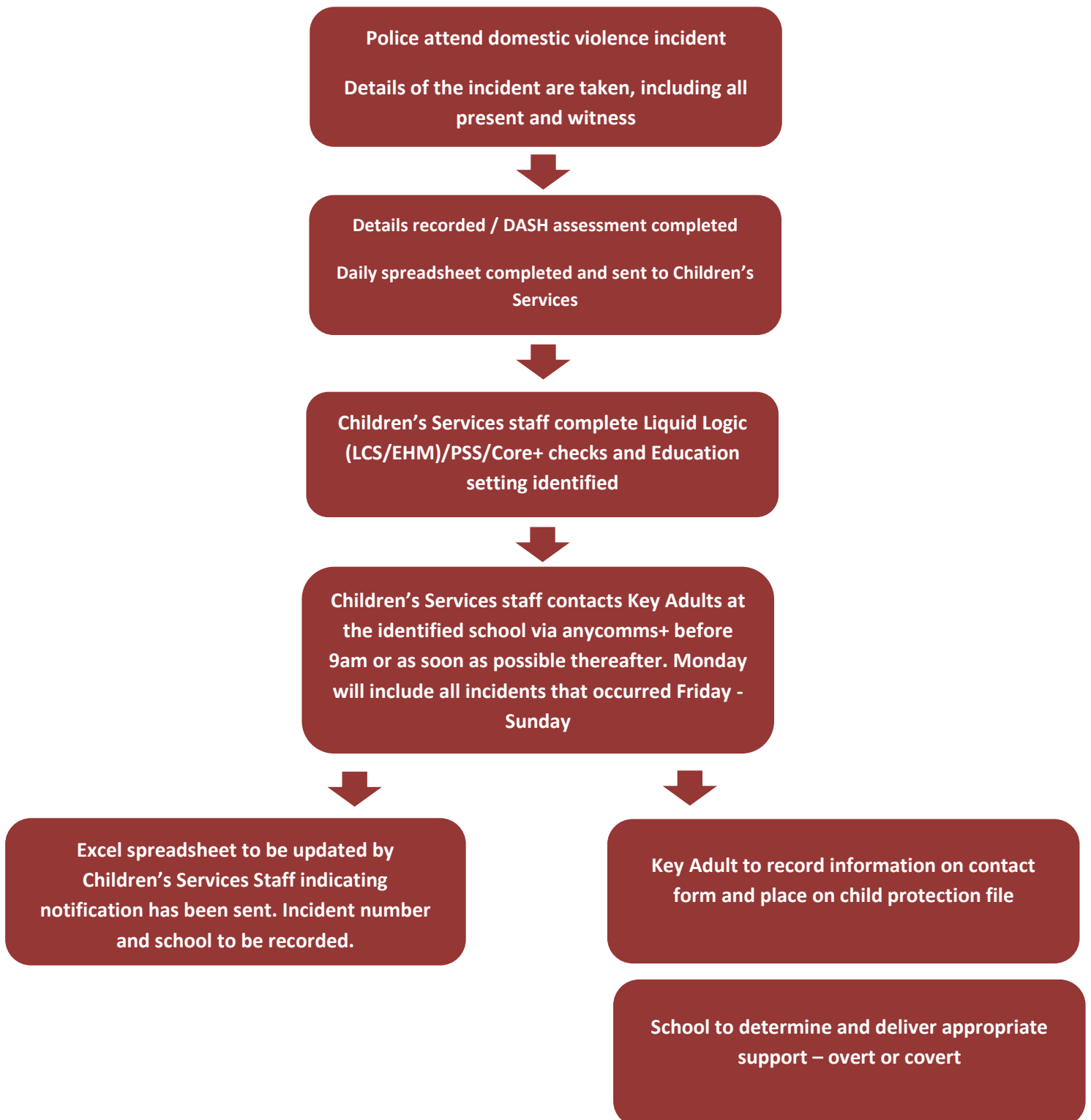
Signature: .....

Name:

Date:

**Notification process for schools for Domestic Abuse & Violence incidents**

This process intends to notify schools before 9am or as soon as possible thereafter where a child has been witnessing, present or involved in a domestic incident, where police have attended. This process does not replace existing child protection / safeguarding arrangements.



### Operation Encompass Agreement

Operation Encompass is a joint operation between Norfolk Children's Services, Norfolk Police and School. It has been established to provide schools with notification of domestic incidents that have occurred the previous day before 9am the following morning. This enables schools to provide timely support to the children and their families. To enable schools to start receiving notifications they must have;

- Read and agreed to the Information Sharing Agreement
- Provide at least 2 nominated members of staff to be Key Adults, they must be Designated Safeguarding Trained and have attended the Operation Encompass Briefing.
- Inform [operationencompass@norfolk.gov.uk](mailto:operationencompass@norfolk.gov.uk) when a Key Adult leaves the school.
- Informed all parents of the school about their intentions to be part of Operation Encompass.

Please complete the form below and return via email to [operationencompass@norfolk.gov.uk](mailto:operationencompass@norfolk.gov.uk)

<b>Name</b>	
<b>Job title</b>	
<b>School</b>	
<b>Contact Number</b>	(Please include direct dials/mobile numbers if applicable)
<b>Email</b>	(Please provide work email address for AnyComms user account)

*I confirm that I have read and agreed to the information Sharing Agreement.*

*I confirm that the school has sent the letter provided to all parents / carers informing them of the school's intentions to participate in Operation Encompass.*

*I confirm that I understand the sensitive nature of the information I may receive regarding children young people and their families as part of operation Encompass and agree that the school is responsible for the appropriate sharing of that information thereafter.*

**Name:**

**Job Title:**

**Signature:**

**Date:**

OFFICIAL