

INFORMATION SHARING

CONTENTS

1. Introduction
2. Information sharing myth busting
3. Legislation and Guidance
4. The Seven Golden Rules for Information Sharing
5. Information requested by NEL SCP for the Purpose of its functions

1. INTRODUCTION

Working Together to Safeguard Children 2018 states for Information Sharing:

Effective sharing of information between practitioners and local organisations and agencies is essential for early identification of need, assessment and service provision to keep children safe. Serious case reviews (SCRs13) have highlighted that missed opportunities to record, understand the significance of and share information in a timely manner can have severe consequences for the safety and welfare of children.

Practitioners should be proactive in sharing information as early as possible to help identify, assess and respond to risks or concerns about the safety and welfare of children, whether this is when problems are first emerging, or where a child is already known to local authority children's social care (e.g. they are being supported as a child in need or have a child protection plan). Practitioners should be alert to sharing important information about any adults with whom that child has contact, which may impact the child's safety or welfare.

Information sharing is also essential for the identification of patterns of behaviour when a child has gone missing, when multiple children appear associated to the same context or locations of risk, or in relation to children in the secure estate where there may be multiple local authorities involved in a child's care. It will be for local safeguarding partners to consider how they will build positive relationships with other local areas to ensure that relevant information is shared in a timely and proportionate way.

Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare, and protect the safety, of children, which must always be the paramount concern. To ensure effective safeguarding arrangements:

- all organisations and agencies should have arrangements in place that set out clearly the processes and the principles for sharing information. The arrangement should cover how information will be shared within their own organisation/agency; and with others who may be involved in a child's life.
- all practitioners should not assume that someone else will pass on information that they think may be critical to keeping a child safe. If a practitioner has concerns about a child's welfare and considers that they may be a child in need or that the child has suffered or is likely to suffer significant harm, then they should share the information with local authority children's social care and/or the police. All practitioners should be particularly alert to the importance of sharing information when a child moves from one local authority into another, due to the risk that knowledge pertinent to keeping a child safe could be lost
- all practitioners should aim to gain consent to share information but should be mindful of situations where to do so would place a child at increased risk of harm. Information may be shared without consent if a practitioner has reason to believe that there is good reason to do so, and that the sharing of information will enhance the safeguarding of a child in a timely manner. When decisions are made to share or withhold information, practitioners should record who has been given the information and why

Practitioners must have due regard to the relevant data protection principles which allow them to share personal information, as provided for in the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). To share information effectively:

- all practitioners should be confident of the processing conditions under the Data Protection Act 2018 and the GDPR which allow them to store and share information for safeguarding purposes, including information which is sensitive and personal, and should be treated as 'special category personal data'
- where practitioners need to share special category personal data, they should be aware that the Data Protection Act 2018 contains 'safeguarding of children and individuals at risk' as a processing condition that allows practitioners to share information. This includes allowing practitioners to share information without consent, if it is not possible to gain consent, it cannot be reasonably expected that a practitioner gains consent, or if to gain consent would place a child at risk.

2. INFORMATION SHARING MYTH BUSTING

Working Together to Safeguard Children 2018 provides the following Myth-busting guide to information sharing:

Sharing information enables practitioners and agencies to identify and provide appropriate services that safeguard and promote the welfare of children. Below are common myths that may hinder effective information sharing.

Data protection legislation is a barrier to sharing information

No – the Data Protection Act 2018 and GDPR do not prohibit the collection and sharing of personal information, but rather provide a framework to ensure that personal information is shared appropriately. In particular, the Data Protection Act 2018 balances the rights of the information subject (the individual whom the information is about) and the possible need to share information about them.

Consent is always needed to share personal information

No – you do not necessarily need consent to share personal information. Wherever possible, you should seek consent and be open and honest with the individual from the outset as to why, what, how and with whom, their information will be shared. You should seek consent where an individual may not expect their information to be passed on. When you gain consent to share information, it must be explicit, and freely given. There may be some circumstances where it is not appropriate to seek consent, because the individual cannot give consent, or it is not reasonable to obtain consent, or because to gain consent would put a child's or young person's safety at risk.

Personal information collected by one organisation/agency cannot be disclosed to another

No – this is not the case, unless the information is to be used for a purpose incompatible with the purpose for which it was originally collected. In the case of children in need, or children at risk of significant harm, it is difficult to foresee circumstances where information law would be a barrier to sharing personal information with other practitioners.

The common law duty of confidence and the Human Rights Act 1998 prevent the sharing of personal information

No – this is not the case. In addition to the Data Protection Act 2018 and GDPR, practitioners need to balance the common law duty of confidence and the Human Rights Act 1998 against the effect on individuals or others of not sharing the information.

IT Systems are often a barrier to effective information sharing

No – IT systems, such as the Child Protection Information Sharing project (CP-IS), can be useful for information sharing. IT systems are most valuable when practitioners use the shared data to make more informed decisions about how to support and safeguard a child.

3. LEGISLATION AND GUIDANCE

THE DATA PROTECTION ACT 2018 / GENERAL DATA PROTECTION REGULATION (GDPR):

The Data Protection Principles requires that personal data shall be:

NORTH EAST LINCOLNSHIRE SAFEGUARDING CHILDREN PARTNERSHIP

- a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')
- b) 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 not be considered to be incompatible with the initial purposes ('purpose limitation')
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- d) 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) 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation')
- f) 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').

The Data Protection Act and GDPR also provides individuals with the following rights in relation to their personal data:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

CALDICOTT GUARDIAN PRINCIPLES:

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing. The Guardian plays a key role in ensuring that the NHS, Local Authority Social Services Departments and partner organisations satisfy the highest practicable standards for handling patient identifiable information.

The Seven Caldicott Principles are:

1. Justify the purpose(s) for using confidential information
2. Don't use personal confidential data unless it is absolutely necessary
3. Use the minimum necessary personal confidential data
4. Access to personal confidential data should be on a strict need-to-know basis
5. Everyone with access to personal confidential data should be aware of their responsibilities; 6. Comply with the law
6. The duty to share information can be as important as the duty to protect patient confidentiality.

NORTH EAST LINCOLNSHIRE SAFEGUARDING CHILDREN PARTNERSHIP

These are applicable to children's services and health services. They have more recently been extended into councils with social care responsibilities, in order to provide a framework for working within the Data Protection Act and to promote appropriate information sharing.

Every local Health Service and children's services has its own Caldicott Guardian, to provide advice and guidance on appropriate information sharing.

For North East Lincolnshire Council, the Caldicott Guardian is Stephen Pintus who can be contacted on transparency@nelincs.gov.uk

SECTION 115 OF THE CRIME AND DISORDER ACT 1998 ESTABLISHES

The power to disclose information is central to the Act's partnership approach. The Police have an important general power under common law to disclose information for the prevention, detection and reduction of crime. However, some other public bodies that collect information may not previously have had power to disclose it to the Police and others. This section puts beyond doubt the power of any organisation to disclose information to Police authorities, local authorities, Probation Provider, Health Authorities, or to persons acting on their behalf, so long as such disclosure is necessary or expedient for the purposes of crime prevention. These bodies also have the power to use this information.

THE DOMESTIC VIOLENCE DISCLOSURE SCHEME

The Domestic Violence Disclosure Scheme (DVDS) commenced on 8 March 2014. The DVDS gives members of the public a formal mechanism to make enquires about an individual who they are in a relationship with, or who is in a relationship with someone they know, where there is a concern that the individual may be violent towards their partner. This scheme adds a further dimension to the information sharing about children where there are concerns that domestic violence and abuse is impacting on the care and welfare of the children in the family.

Members of the public can make an application for a disclosure, known as the 'right to ask'. Anybody can make an enquiry, but information will only be given to someone at risk or a person in a position to safeguard the victim. The scheme is for anyone in an intimate relationship regardless of gender.

Partner agencies can also request disclosure is made of an offender's past history where it is believed someone is at risk of harm. This is known as 'right to know'.

SECTION 115 OF THE CRIME AND DISORDER ACT 1998 ESTABLISHES

The power to disclose information is central to the Act's partnership approach. The Police have an important general power under common law to disclose information for the prevention, detection and reduction of crime. However, some other public bodies that collect information may not previously have had power to disclose it to the Police and others. This section puts beyond doubt the power of any organisation to disclose information to

Police authorities, local authorities, Probation Provider, Health Authorities, or to persons acting on their behalf, so long as such disclosure is necessary or expedient for the purposes of crime prevention. These bodies also have the power to use this information.

THE DOMESTIC VIOLENCE DISCLOSURE SCHEME

The Domestic Violence Disclosure Scheme (DVDS) commenced on 8 March 2014. The DVDS gives members of the public a formal mechanism to make enquires about an individual who they are in a relationship with, or who is in a relationship with someone they know, where there is a concern that the individual may be violent towards their partner. This scheme adds a further dimension to the information sharing about children where there are concerns that domestic violence and abuse is impacting on the care and welfare of the children in the family.

NORTH EAST LINCOLNSHIRE SAFEGUARDING CHILDREN PARTNERSHIP

Members of the public can make an application for a disclosure, known as the 'right to ask'. Anybody can make an enquiry, but information will only be given to someone at risk or a person in a position to safeguard the victim. The scheme is for anyone in an intimate relationship regardless of gender.

Partner agencies can also request disclosure is made of an offender's past history where it is believed someone is at risk of harm. This is known as 'right to know'.

If a potentially violent individual is identified as having convictions for violent offences, or information is held about their behaviour which reasonably leads the police and other agencies to believe they pose a risk of harm to their partner, a disclosure will be made.

For further information see the **Metropolitan Police website**.

ARTICLE 8 IN THE EUROPEAN CONVENTION ON HUMAN RIGHTS STATES THAT

Everyone has the right to respect for his/her private and family life, home and correspondence.

There shall be no interference by a public authority with the exercise of this right except such as 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 rights and freedoms of others.

AGE ASSESSMENT INFORMATION SHARING FOR UNACCOMPANIED ASYLUM SEEKING CHILDREN

The issue of age assessment in social work with asylum seeking young people remains controversial and has been something that Children's social care have struggled with since the millennium. The ADCS Asylum Task Force has worked with the Home Office to provide two new jointly agreed documents, as detailed below. These documents are offered as practice guidance, by way of assistance to local authorities and their partners. The use of the proforma and consent form is voluntary. The content does not, nor does it seek to, be binding on local authorities. It is simply a recommended approach.

See **ADCS Age Assessment Information Sharing for UASC**.

CHILD SEX OFFENDER DISCLOSURE SCHEME

The Child Sex Offender Review (CSOR) Disclosure Scheme is designed to provide members of the public with a formal mechanism to ask for disclosure about people they are concerned about, who have unsupervised access to children and may therefore pose a risk. This scheme builds on existing, well established third-party disclosures that operate under the Multi-Agency Public Protection Arrangements (MAPPA).

Police will reveal details confidentially to the person most able to protect the child (usually parents, carers or guardians) if they think it is in the child's interests.

The scheme has been operating in all 43 police areas in England and Wales since 2010. The scheme is managed by the Police and information can only be accessed through direct application to them.

If a disclosure is made, the information must be kept confidential and only used to keep the child in question safe. Legal action may be taken if confidentiality is breached. A disclosure is delivered in person (as opposed to in writing) with the following warning:

- 'That the information must only be used for the purpose for which it has been shared i.e. in order to safeguard children
- The person to whom the disclosure is made will be asked to sign an undertaking that they agree that the information is confidential and they will not disclose this information further.

- A warning should be given that legal proceedings could result if this confidentiality is breached. This should be explained to the person and they must sign the undertaking' (Home Office, 2011, p16).

If the person is unwilling to sign the undertaking, the police must consider whether the disclosure should still take place.

4. THE SEVEN GOLDEN RULES FOR INFORMATION SHARING

There are seven golden rules for information sharing which should be followed by all organisations working with and providing services for children and their families: (see **Information sharing: advice for practitioners providing safeguarding services (July 2018)**).

1. Remember that the Data Protection Act and human rights laws are not barriers to justified information sharing but provide a framework to ensure that personal information about living individuals is shared appropriately
2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so
3. Seek advice from other practitioners if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible
4. Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, there is good reason to do so, such as where safety may be at risk. You will need to base your judgment on the facts of the case. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to be shared
5. Consider safety and well-being: Base your information sharing decisions on considerations of the safety and wellbeing of the individual and others who may be affected by their actions
6. Necessary, proportionate, relevant, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (Practitioners must always follow their organisation's policy on security for handling personal information)
7. Keep a record of your decision and the reasons for it - whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Source: **Information sharing: advice for practitioners providing safeguarding services (July 2018)**.

Each situation should be considered on a case-by-case basis. Professionals should always seek advice from senior colleagues, including the Data Protection Officer and legal services, where clarity is required.

5. INFORMATION REQUESTED BY THE NEL SCP FOR THE PURPOSE OF ITS FUNCTIONS

Every NEL SCP should play a strong role in supporting information sharing between and within organisations and addressing any barriers to information sharing. This should include ensuring that a culture of information sharing is developed and supported as necessary by multi-agency training.

The core legislation underpinning the work of the NEL SCP is the Children Act 2004, which provides a comprehensive framework for the care and protection of children. Detailed statutory guidance is also contained in Working Together to Safeguard Children 2015.

Under section 14B of the Children Act 2004, the NEL SCPB can require a person or body to comply with a request for information. This can only take place where the information requested is for the purpose of enabling or assisting the NEL SCP to perform its functions. This includes information required in respect of the Serious Case Review, Child

Death Review and the Allegations Management Any request for information about individuals must be necessary and proportionate to the reasons for the request. The NEL SCP should be mindful of the burden of requests and should explain why the information is needed.

INFORMATION REQUESTED BY THE NEL SCP FROM SCHOOLS AS PART OF THE ALLEGATIONS

MANAGEMENT PROCESS

NEL SCP will make requests for information from the School Children Protection Officer (SCPO). The request will be made by secure e-mail to the SCPO, where this facility is not available the request will be sent in an encrypted or password protected document. Passwords will be provided to SCPO under separate arrangements.

When making a request for information about individuals, the Safeguarding unit will only ask for the information that is 'necessary' and 'proportionate' to the purposes of the NEL SCP as allowed by section 14B of the Children Act 2004.

ANSWERING REQUESTS FOR INFORMATION MADE ON BEHALF OF THE NEL SCPB

School Children Protection Officer (SCPO) should answer the requests by secure e-mail / MoveIT, where this facility is not available the response should be sent in an encrypted or password protected document. Passwords must be provided to the Safeguarding unit under separate arrangements.

Secure transfer of NEL SCP information. NEL SCP information will be transferred to School Children Protection Officer either at NEL SCP meetings or by secure e-mail, where this facility is not available the response should be sent in an encrypted or password protected document, with passwords provided to under separate arrangements.

SECURITY AND PROTECTION OF NEL SCPB INFORMATION

Schools must ensure that all NEL SCP case records are kept secure and protected at all times to prevent unauthorised access or loss. Clear screen and desk policies should be in place. Information should be stored in folders restricted to authorised users, or in locked storage areas or cabinets. Encrypted USBs can be used for the purpose of secure transportation, but not long-term storage. Documents taken out of the secure environment must be placed in closable folders, and remain with the designated officer at all times, they must never be left unattended.

Retention and disposal of NEL SCP case records: The primary records for the NEL SCP will be held by North East Lincolnshire Council's Safeguarding unit. The records held by schools will be secondary records and should be retain for as long as is necessary to meet their business requirements. In most cases this should be no longer than the school year following the 25th birthday of the pupil. All NEL SCPB case records held by schools must be disposed of by controlled secure methods, it is recommended that this is either by cross cut shredding or incineration.

CORPORATE PARENTING - LOOKED AFTER CHILDREN

Where North East Lincolnshire Council is the 'corporate parent' for the looked after children in its care, they will receive the same information in relation to the child's education from the school as would any other parent or guardian with parental responsibility for a child. North East Lincolnshire Council will not seek from the school any information it is not entitled to.