Information-Sharing Code of Practice

For Cause for Concern and Safeguarding

Middlesex University

Author - Ben Serlin

Approved – Safeguarding Board, September 2016

Date for review – September 2017

This code of practice is to enable effective sharing of information within Middlesex University and externally by Designated Safeguarding Officers and other members of the Safeguarding-Cause for Concern team.

Contents

1. Introduction

1.1 This document is applicable to all Designated Safeguarding Officers and members of the Safeguarding-Cause for Concern team, referred to collectively in this code of practice as Designated Safeguarding Officers (DSOs). Safeguarding and cause for concern is collectively referred to in this code of practice as safeguarding.

1.2 The code of practice is not a legally binding document. It details the arrangements, processes, and the principles for sharing information internally and externally in the context of safeguarding.

1.3 The code of practice has been developed to define the specific purposes for which information is to be shared internally within Middlesex University and externally with, for example, Local Safeguarding Boards, Local Authorities and Practitioners. In doing so, it aims to promote a consistent approach to information sharing.

1.4 The code of practice details the reasons for information sharing; the responsibilities and commitments of DSOs to this agreement, and; the arrangements for monitoring and review. It provides a summary of the legal gateway through which information is shared, including reference to the Human Rights Act (1998) and the Common Law Duty of Confidentiality, and the security procedures necessary to ensure compliance with responsibilities under the Data Protection Act (1998).

1.5 The code of practice complies with the general principles of information sharing as set out in the University's Information Sharing Policy. It aligns with all other codes of practices, protocols, and policies to which DSOs may already be signatories, and does not in any way supersede those existing agreements.

1.6 It is not intended that this document be definitive or exhaustive: it is recognised that as policy develops and implementation arrangements mature, this code of practice will need to be reviewed and amended in light of new information sharing requirements to ensure that it remains 'fit for purpose'.

2. Purpose of the Code of Practice

2.1 The overarching aim of this code of practice is to support the successful delivery of safeguarding for all students and staff at Middlesex University by facilitating and governing the efficient, effective and secure sharing of good quality information.

2.2 The code of practice endeavours to ensure all DSOs are empowered and committed to share good quality and relevant information, and that all information is consistently shared in an appropriate, secure and fair way, at the right time, with the right people. It aims to ensure all DSOs understand the importance of sharing information, the potential risks of not sharing it, and to understand when to raise a concern with external agencies.

2.3 As information sharing can be complex and sometimes confusing for staff, this code of practice sets out to clarify the channels of communication, policies and procedures underpinning the sharing of information, to ensure all DSOs feel confident about sharing information relating to safeguarding.

2.4 The code of practice is to support effective decision-making by providing a useful tool in enabling communication and collaboration internally between DSOs, and externally with agencies.

3. Why is information sharing important?

3.1 'Information sharing is vital to safeguarding and promoting the welfare of children and young people. A key factor identified in many serious case reviews has been a failure by practitioners to record information, to share it, to understand its significance and then take appropriate action' *(Information Sharing – Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers, March 2015)*.

3.2 Appropriate and timely sharing of relevant information is a vital part of the early intervention approach promoted at Middlesex University. The decisions about how much information to share, with who, and when, can improve outcomes for all, have a profound impact on the lives of individuals, and help prevent situations from escalating into tragedies.

3.3 Serious case reviews routinely show that no single service had a full, clear picture about what was going on in a child's life. Early indications of a threat to wellbeing had been missed, or hadn't been responded to at the earliest opportunity. This is also true of adults at risk with adult serious case reviews frequently highlighting failures between safeguarding partners (local authorities, GPs and health practitioners, the police, housing, care providers) to communicate and work jointly. Such failures have led to serious abuse and harm, and in some cases, death.

3.4 Good quality information sharing is necessary:

- To prevent or reduce risk, serious harm or death, and promote wellbeing.
- To help students and staff to access the right kind of support and services at the right time.
- To enable early interventions which are likely to have better outcomes for an individual by prevent the escalation of risk, avoiding the need for a higher level of care and support.
- To reveal patterns of abuse that were previously undetected and that could identify others at risk.
- To identify low-level concerns that may reveal people at risk of abuse.
- To help identify people who may pose a risk to others and, where possible, to work to reduce offending behaviour.

3.5 Effective information-sharing is also fundamental to reducing organisational risk and protecting the University's reputation.

4. The Legislative Framework

4.1 The legislative framework is not a barrier to information sharing, but serves to provide a framework to ensure that personal information is shared appropriately.

4.2 Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of individuals at risk of abuse or neglect. It is important that all DSOs feel confident about when and how information can be shared legally.

4.3 All information shared under the terms of this code of practice must be done so in compliance with the following legislation:

- The Data Protection Act (1998)
- Common Law Duty of Confidentiality
- The Human Rights Act (1998), notably Article 8 (the right to respect for private life)
- The Crime and Disorder Act (1998)
- The Mental Capacity Act (2005)
- Safeguarding Law

4.4 The Data Protection Act (1998)

i. The University treats all personal and sensitive data according to the Data Protection Act (1998) and in line with the University's Data Protection Policy. These set out the parameters for sharing information appropriately and safely.

ii. The basic principles are that any personal information should be shared on the basis that:
- It is necessary for the purpose which is being shared.
- It is shared only with those who have a need for it.
- It is accurate and up to date.
- It is shared securely and in a timely fashion.
- It is not kept for longer than necessary for the original purpose: the control of information in respect of individual cases needs to be in accordance with accepted data protection and confidentiality requirements.

iii. The Data Protection Act does not prohibit the collection and sharing of personal information: it provides a framework to ensure that personal information about an individual is shared appropriately. It is important that the Act is not erroneously perceived as a barrier to sharing information, particularly where failure to do so would result in a child or an adult at risk being placed at risk of harm.

iv. The Act balances the rights of the individual and the need to share information about him or her. It is essential to consider this balance in every case and never to assume

sharing is prohibited. For example, 'vital interest' permits sharing of information where it is critical to prevent serious harm or distress, or in life-threatening situations.

v. Personal information collected by one organisation can be disclosed to another organisation as long as the information is to be used for a purpose compatible with the purpose that it was originally collected for. In the case of a child at risk of significant harm, for example, it is difficult to foresee circumstances where sharing personal information would not be compatible with the purpose for which it was originally collected.

4.5 The Common Law Duty of Confidentiality and the Human Rights Act (1998)

i. In addition to considering the Data Protection Act, it is important to balance the Common Law Duty of Confidentiality and the rights within the Human Rights Act (1998) against the effect on individuals or others of not sharing information. The duty to share information can be as important as the duty to protect an individual's confidentiality, right to independence, choice and self-determination, including control over information about themselves.

ii. If information collection and sharing is to take place with the consent (implied or explicit) of the individual involved, providing he or she is clearly informed about the purpose of the sharing, there should be no breach of confidentiality or the Human Rights Act.

iii. The law does not prevent the sharing of sensitive, personal information between organisations. Confidential health information does carry a higher threshold, but it should still be possible to proceed where the circumstances are serious enough.

iv. Confidentiality is an important principle that enables people to feel safe in sharing their concerns and to ask for help. However, the right to confidentiality is not absolute, particularly as good safeguarding practice invariably commands sharing relevant information with the right people at the right time. In fact, a basic principle of safeguarding is that assurances should not be given regarding confidentiality. There, however, must be satisfactory grounds to override the duty of confidentiality.

v. If the information is confidential, but there is a safeguarding concern, sharing it may be justified, even if consent from the individual is not gained. The duty to confidentiality could be overridden, for example, because: it is overwhelmingly in the individual's interests for this information to be disclosed; there is an overriding public interest which justifies the disclosure of the information (such as in an emergency where it may not be appropriate to seek consent for information sharing as it could cause delays and therefore harm to a child or vulnerable adult), or; sharing is required by a court order, other legal obligation or statutory exemption.

vi. Human rights law and concerns should not prevent sharing information where there are real safeguarding concerns. Article 8 of the European Convention on Human Rights, in which individuals have a right to respect for their family and their private lives, is not an absolute right and can be overridden if necessary, in accordance with the law, justified and for a particular purpose. Justification could be the protection of an individual's health, the prevention of crime, or the protection of the rights and freedoms of others.

4.6 The Crime and Disorder Act (1998)

i. Any person may disclose information to a relevant authority under Section 115 of the Crime and Disorder Act (1998), 'where disclosure is necessary or expedient for the purposes of the Act (reduction and prevention of crime and disorder).' 'Relevant authorities' broadly are the police, local authorities, health authorities (clinical commissioning groups) and local probation boards.

ii. The police can keep records on any person known to be a target or perpetrator of abuse and share such information with safeguarding partners for the purposes for protection 'under Section 115 of the Crime and Disorder Act (1998) and the Data Protection Act (1998), provided that criteria outlined in the legislation are met. All police forces now have IT systems in place to help identify repeat and vulnerable victims of antisocial behaviour.

4.7 The Mental Capacity Act (2005)

i. It is necessary to understand and always work in line with the Mental Capacity Act (2005).

ii. The Mental Capacity Act is relevant as all DSOs coming into contact with vulnerable adults will need to use their professional judgement and possibly balance competing views to be able to assess whether that individual has the mental capacity to make a decision concerning risk, safety or sharing information.

4.8 Safeguarding Law

i. Sharing information between organisations as part of day-to-day safeguarding practice is already covered in the Common Law Duty of Confidentiality, the Data Protection Act, the Human Rights Act and the Crime and Disorder Act.

ii. Bodies within the education and/or voluntary sections under section 11 of the Children Act (2004), and any individual to the extent that they are providing services in pursuance of section 74 of the Education and Skills Act (2008), have a duty to have arrangements in place to safeguard and promote the welfare of children.

iii. In addition, the Care Act (2014) places duties on the local authority and its partners to cooperate in the exercise of their functions relevant to care and support including those to protect adults. The Safeguarding Board should ensure that it has the involvement of all partners necessary to effectively carry out its duties.

iv. Section 55 of the Borders, Citizenship and Immigration Act (2009) applies to the immigration, asylum, nationality and customs functions of the Secretary of State (in practice discharged by UK Visas and Immigration, immigration Enforcement and the Border Force, which are part of the Home Office).

v. The Safeguarding Vulnerable Group Act (2006) places specific duties on those providing 'regulated activities'. They must refer to the Disclosure and Barring Service (DBS) anyone who has been dismissed or removed from their role because they are thought to have harmed, or pose a risk of harm to, a child or adult at risk. This applies even if they have left their job and regardless of whether they have been convicted of a related crime.

vi. The London Safeguarding Children Board (LSCB) can require an individual or body to comply with a request for information, as outlined in section 14B of the Children Act (2004). This can only take place when the information requested is for the purpose of enabling or assisting the LSCB to perform its functions. Any requests for information about individuals should be necessary and proportionate to the reason for the request.

vii. DSOs should adhere to the six information sharing principles which underpin good safeguarding, as set out in the Adult Care Act (2014):

- **Empowerment** – to support and encourage people to make their own decisions and informed consent.
- **Prevention** – to endeavour to take action before harm occurs.
- **Proportionality** – to carry out the least intrusive response appropriate to the risk presented.
- **Protection** – to provide support and representation for those in greatest need.
- **Partnership** – to work with the community to prevent, detect and report neglect and abuse**.**
- **Accountability** – to be transparent in safeguarding practice.

4.9 Professional Code of Practice

It is the responsibility of the DSO to ensure that the data sharing transactions undertaken are done so legally and fairly. They must ensure they comply with the legal framework as detailed above and also the professional code of practice as outlined below.

Designated Safeguarding Officers are expected to:

- Understand the need to protect, safeguard and promote the wellbeing of children, young people and vulnerable adults.

- Be able to recognise and respond appropriately to situations where it is necessary to share information to safeguard under-18s and adults at risk.

- Challenge and report dangerous, abusive, discriminatory or exploitative behaviour or practice.

- Adopt best practice akin to a 'critical friend' whereby honest and candid feedback is provided. At times, feedback may be uncomfortable or difficult to hear, particularly when talking about weaknesses, problems, and emotionally charged issues. Therefore, it is important to deliver feedback constructively, in an encouraging and supportive manner, and to receive feedback positively and pro-actively act upon any recommendations.

- Report any actions or omissions by yourself or colleagues that you feel may compromise the safety or care of children or adults at risk and, if necessary, to use whistleblowing procedures to report any suspected wrongdoing, improper or illegal practices, the cover-up of wrongdoing, and/or a neglect of duties. See the University's whistleblowing policy.

- Provide accurate and truthful information. The duty of candour aims to ensure transparency and honesty when things go wrong. It requires DSOs to inform the person concerned as soon as possible when something has gone wrong and to ensure provision of support to them. This will include providing the individual with an apology and keeping them informed about any further enquiries.

6 Information sharing guidelines

6.1 Safeguarding Information Sharing Principles

It is essential that all DSOs apply the following principles when deciding whether or not to share information.

- **Necessary**: when taking decisions about what information to share, consider how much information you need to release. Ensure that the information you share is necessary for the purpose for which you are sharing it and that it is shared only with those individuals who need to have it. You must be able to justify the purpose for sharing information.
- **Proportionate:** consider the impact of disclosing information on the individual and any third parties. Any information shared must be proportionate to the need and level of risk.
- **Relevant and adequate**: information needs to be accurate and up-to-date. DSOs should share, what may appear, small pieces of information. This may allow for patterns to emerge – and these can often point to more serious concerns, allowing appropriate help to be offered at an early stage.
- **Transparent:** DSOs must be open and honest with the individual from the outset about why, what, how and with whom information will, or could be shared, and seek their consent, unless it is unsafe or inappropriate to do so. DSOs must be knowledgeable of issues surrounding confidentiality and consent.
- **Timely**: information should be shared in a timely fashion. DSOs should consider the urgency with which to share it. Timeliness is essential in emergency situations: DSOs should not wait until a situation has reached crisis point before sharing information.
- **Secure:** information must be shared securely.

6.2 The Caldicott Principles

The Caldicott Principles, although designed for the Health and Social Care sector, is an effective tool to guide information sharing in Higher Education. These principles are also reflected in the Data Protection Act (1998):

- Justify the purpose. The information sharing decisions should be based on considerations of the safety and well-being of the individual and others who may be affected by their actions.
- Do not use personal confidential data unless it is absolutely necessary.
- Use the minimum personal confidential data necessary for purpose.
- Access to personal confidential data should be on a strict need-to-know basis.
- Everyone with access to personal confidential data should be aware of their responsibilities.
- Comply with the law.
-

6.2 Working in collaboration

i. No DSO is to work in isolation. It is imperative that all DSOs discuss each case with another DSO, to work in collaboration to address concerns, and to carry out effective resolutions.

ii. All DSOs should be alert to the signs and triggers of abuse and neglect to under-18s and adults at risk. Abuse (emotional, physical, sexual and financial) and neglect can present in many different forms. Children may disclose abuse: in which case the decision to share information is clear. In other cases, for example, neglect, the indicators may be more subtle and appear over time. In these cases, decisions about what information to share, and when, will be more difficult to judge and it is therefore essential that DSOs work in collaboration to determine which information to share.

iii. Middlesex University members of staff who are not a DSO should always report safeguarding concerns in line with University policy to a DSO. DSOs should remind staff that they should not disclose the identity of the individual where possible. DSOs should encourage the staff member to discuss the case as a hypothetical scenario but not to disclose information until it has been decided a suitable way forward. DSOs are in the best position to use professional judgement about when to share information with colleagues working within Middlesex University, as well as with those working within other organisations.

iv. DSOs should not assume that someone else will pass on information which may be critical to keeping an under-18 or adult at risk safe.

6.3 Sharing information externally

i. It is good practice, unless there are clear reasons for not doing so, to work with the carers, family and friends of under-18s or adults at risk to help them to get the care and support they need. Sharing information with these people should always be with consent of the individual.

ii. If it is thought that a crime has been committed and/or an individual is at immediate risk, the police should be notified without delay.

iii. The Safeguarding Board has a key role to play in sharing information and intelligence on patterns and trends within the organisation. The Board's annual report must provide information about any safeguarding reviews. This can include learning to inform future prevention strategies.

7 Consent

7.1 Information sharing with consent

- Before any information is shared, you should seek consent from the individual. Where possible the individual should be in control of how much information is shared and with whom.
- You should endeavour to copy the individual into any such correspondence so that the individual is aware of any information which is shared.
- Specific details about an individual should only be passed to other people with the individual's consent unless the threshold for sharing information without consent is met.

7.2 When to share information without consent

It is possible to share personal information without consent (explicit or implied). In situations relating to safeguarding, there are numerous circumstances where it would be acceptable to share information.

- If it is necessary to protect the vital interests of the individual where, for example, it is not possible for consent to be given.
- If it is in the 'public interest' for information to be shared.
- If there is an emergency or life-threatening situation, relevant information may be shared with the relevant emergency services without consent.
- If there is a perceived risk of harm to the individual or if other individuals, particularly children or vulnerable adults, are at risk.
- If the individual does not have the mental capacity to make the decision and/or fully understand the possible consequences. Overriding the individual's decision should be properly explored and recorded in line with the Mental Capacity Act.
- If the individual is under duress or being coerced.
- If the frequency and seriousness of abuse is perceived to warrant intervention.
- If staff are implicated.
- If sharing information can prevent a crime. If someone says they are going to commit a crime, you have a duty to report it. Information relating to certain crimes, notably drugs, trafficking and money laundering, may potentially be shared without consent.
- If a court order or other legal authority has requested the information.
- If the referred case potentially falls under the Prevent Duty. The Prevent Duty sets out a legal obligation whereby information must be forwarded without consent. See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445916/Prevent_Duty_Guidance_For_Higher_Education__England__Wales_.pdf

- If it is unsafe or inappropriate to do so, i.e. where there are concerns that a child is suffering, or is likely to suffer significant harm.

7.3 If there are sufficient grounds to share information, and consent is not granted

- Try to understand the reasons why consent is not given. Explore the reasons for the individual's objections, and address their concerns. They may not give consent for a number of reasons, such as being frightened of reprisals, a fear of losing control, a lack of trust of social services, or a fear that their relationship with an abuser may be damaged.
- Explain why you think it is important to share the information.
- Explain the benefits to them or others of sharing information. For example, if the information is shared, the individual will be able to access better help and support
- Discuss the consequences of not sharing the information, for example, someone could come to harm.
- Tell the individual who you would like to share the information with and why.
- Reassure the individual that the information will not be shared with anyone who does not need to know.
- Reassure the individual that they are not alone and that support is available to them.
- Use gentle persuasion, explaining what help and/or protection might be available. People can often be persuaded to accept help or intervention if they know that they can remain in control of decision-making and care will be taken to maintain relationships.

7.4 The decision to share information without consent

- When deciding whether to share information without consent, it is important to talk to a DSO partner. DSOs should discuss cases as hypothetical situations at first, therefore avoiding the need to reveal information which identifies the individual concerned. A decision can then be made as to whether full disclosure is necessary without the consent of the person concerned.
- If it is decided that the information should be shared, you should talk through the implications to the individual of not sharing information (see 7.3).
- If the decision is made that the information should be shared, and the individual cannot be persuaded to give their consent, you should explain to the individual how the information will be shared and with whom. The reasons for sharing information without consent should also be given to the individual.
- If it is considered dangerous to explain to the individual that information is to be shared without consent, or if it puts any individuals at significant risk, you should consider not informing the individual.
- You must record the decision to share information and the reasoning behind that decision in your case-notes, along with what information was shared.
- The safeguarding principle of proportionality should underpin decisions about sharing information without consent, and decisions should be made on a case-by-case basis.

7.5 When not to share information without consent

If the individual does not give consent and there are insufficient grounds to share the information, then the information should not be shared. Below is a list of some scenarios which in which it would not be appropriate to share information without consent.

- If nobody else is at risk.
- If a serious crime has not been or will not be committed.
- If the alleged abuser has no care and support needs.
- If no staff are implicated.
- If no coercion or duress is suspected.
- If the public interest served by the disclosure does not outweigh the public interest served by protecting confidentiality.
- If the police or other legal authority have not requested the information.

7.6 The risk of sharing information

i. It is important that the risk of sharing information is also considered.

ii. In some cases, such as domestic violence or hate crime, it is possible that sharing information could increase the risk to the individual. DSOs need to work jointly to provide advice, support and protection to the individual in order to minimise the possibility of worsening the relationship or triggering retribution from the abuser. DSOs should work closely with Children and Adult Social Care services with regards to this.

iii. Enquiries should be made to establish whether the individual has care or support needs, or is a Carer, to inform decision-making on whether or not to refer.

7.7 If consent is not granted and there are insufficient grounds to share information

- Support the individual to weigh up the risks and benefits of different options.
- Ensure they are aware of the level of risk and possible outcomes.
- Agree on and record the level of risk the person is taking.
- Record the reasons for not intervening or sharing information.
- Build trust and use gentle persuasion to enable the person to better protect themselves.
- Offer support for them to build confidence and self-esteem if necessary, or try to connect them with somebody who could provide support, for example a Resident Assistant or classmate.
- Regularly review the situation.

8. Record keeping

8.1 Recording information

i. If you have concerns about the welfare or safety of an individual, it is vitally important to record all relevant details, regardless of whether or not the information is shared.

ii. If a decision is made to share information, then a record should be recorded of what has been shared, with whom and for what purpose.

iii. If you decided not to share the information, you must state the reasons why that decision was taken.

iv. If the individual is unaware of the record's existence, record the reasons why you have not told them.

v. Although Individual events may appear to be insignificant 'one-offs', they enable a more accurate picture of a case; they detail the history of a service user and their family; they may indicate a pattern; they highlight gaps and missing details, and; they identify risks, concerns, themes, strengths, resilience and weaknesses of an individual. All which may lead to further action and/or intervention. You should record individual events in chronological order.

vi. An accurate record should include the following:

- Date and time when the report was written.
- A synopsis of any discussion(s) (face to face; telephone; email, meetings etc.).
- The date and time of incident(s)/disclosure(s), a list of any parties involved, including any witnesses to an event, and notes on what was said or done by whom.
- Any interpretation/inference drawn from what was observed, said or alleged. If you express your opinion, you must clearly distinguish between fact and opinion and explain the reasons why you have arrived at that opinion.
- The source of the knowledge, if you are repeating information given to you. If information is historical then this should be explained.

Remember, records should be as meaningful in 20 years' time as they are at the time of writing.

8.2 Retention, storage and destruction of records

i. The Middlesex University Record Management Policy covers the retention, storage and destruction of records. However, some important principles are detailed below.

ii. Security of information sharing must always be considered and should be proportionate to the sensitivity of the information and circumstances.

iii. Access to safeguarding records should be limited to people in named roles who either need to know about the information in those records and/or who manage the records/files.

iv. Sensitive information must not be kept on general access. Paper files containing sensitive or confidential data must be shared in a secure location. All electronic recorded information must be password protected. Neither paper nor electronic files should be left unattended, for example, on public transport or in a public place.

v. Records should be retained even if the information received was judged to be malicious, unfounded or erroneous.

vi. The Data Protection Act, in Guidance to Social Services (2000), asserts that the normal period for the storage of personal information should not exceed 6 years after the individual's last contact with the university. When records are kept for more than 6 years, files need to be clearly marked with the reasons for the extension period be clearly identified.

9. Quick Guide

Ask the following questions to help decide whether or not to share information if you have concerns about the welfare or safety of an individual.

Is there a clear and legitimate purpose for information sharing?

(yes = see next question; no = do not share)

Does the information enable an individual to be identified?

(yes = see next question; no = you can share but you should consider how)

Is the information confidential?

(yes = see next question; no = you can share but you should consider how)

Do you have consent?

(yes = you can share but you should consider how; no = see next question)

Is there another reason to share information? (e.g. to fulfil a public function or protect the vital interests of the individual). *(yes = you can share but consider how; no = do not share)*

Points to remember:

- Record the decision whether to share the information or not. Your decision must be in line with the legal framework and Middlesex University policies, as detailed in this code of practice.
- Always work in collaboration with another DSO and seek further advice if unsure.
- If there are concerns that a child or adult at risk is suffering or likely to suffer harm then it is vital that you follow the relevant procedures without delay.

When sharing information:

- Identify how much information to share.
- Distinguish fact from opinion.
- Ensure that you are giving the right information to the right individual.
- Ensure where possible that you are sharing the information securely.
- Inform the individual that the information has been shared if they were not aware of this as long as this would not create or increase risk of harm.