Bexley Safeguarding Children Board

Information Sharing and Secure Document Transfer Guidance

All professionals who work with children and young people, or with adults who are parents or carers, should know how and when to share information with other professionals in order to keep children safe.

May 2015

With acknowledgement to Wandsworth Safeguarding Children Board

Seven Golden Rules for Information Sharing

Some professionals worry about their responsibility to keep information private under the Data Protection Act 1998 (external link) - but there are simple ways to make sure you share information appropriately:

1. Remember that the Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.
2. Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. Seek advice if you are in any doubt, without disclosing the identity of the person where possible.
4. Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.
5. Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the person 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.
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.

Information Sharing Resources

Evidence from the majority of child protection tragedies and much of the learning from Serious Case Reviews shows that ineffective or lack of information sharing is a key factor.

Guidance is also available on the BSCB website:
http://www.bexleylscb.org.uk/page.php?section=section_5&id=267#Information sharing

Some points to remember about information sharing are:

- **Never assume** that other professionals are taking the action you would expect - check with them directly.
- **Check your terminology** - as professionals, we all use our own jargon and 'short-hand' - this makes things easier between ourselves, but can confuse people who are not familiar with our language. Make sure that you are clear, especially when working with professionals in other disciplines.
- **Get feedback** - find out what action another professional will take as a result of the information you have given them, and verify that it has taken place.

Sharing information where there are concerns about Significant Harm

Professionals working with children, parents or adults in contact with children, should always share information with children's social care where there is reasonable cause to suspect that a child may be suffering or is at risk of suffering significant harm. Sharing information under these circumstances is legitimate and in the public interest.

Deciding whether personal and/or sensitive information can be shared

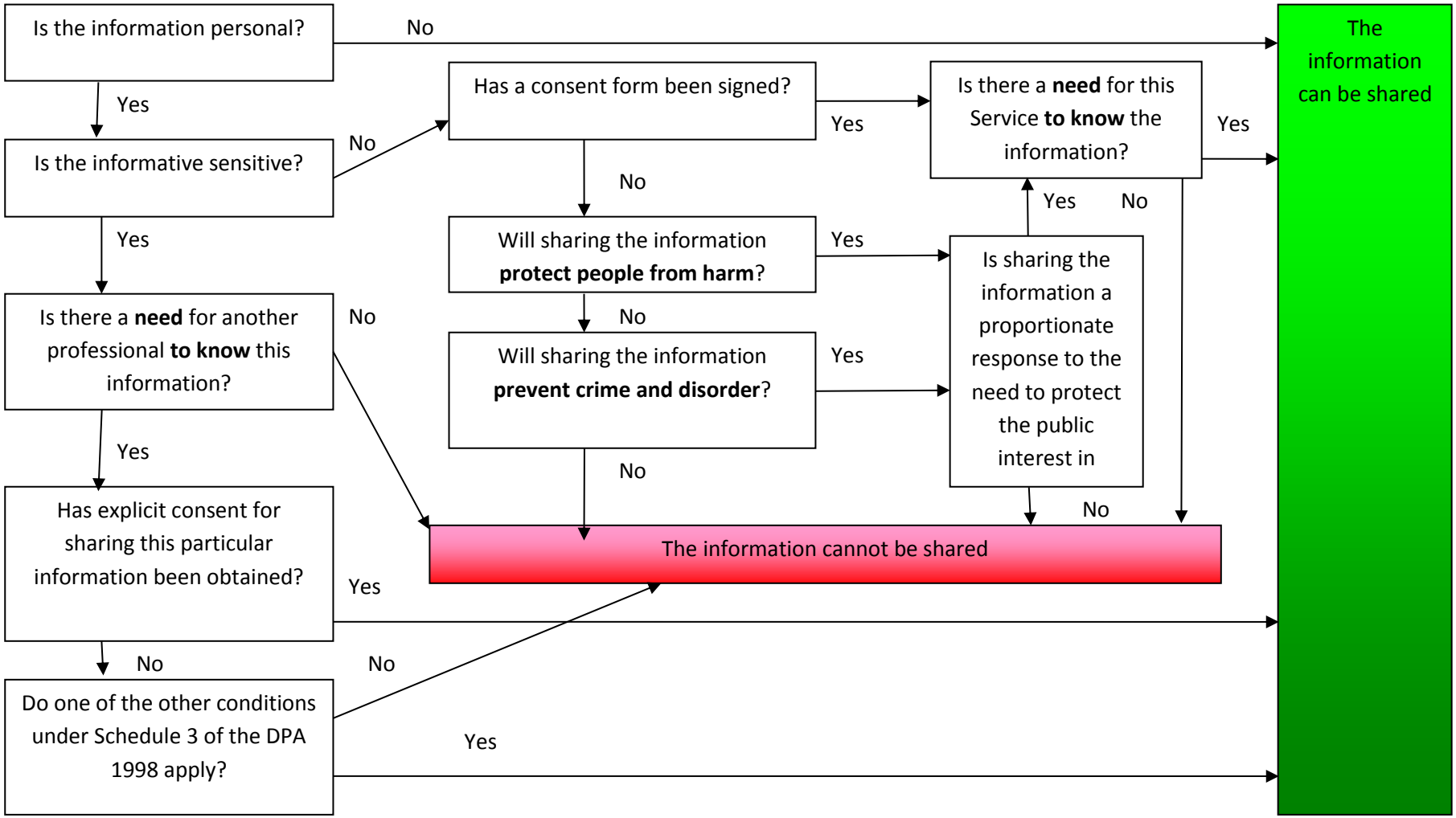
Can we share information?

Yes. But different types of information have different rules that must be followed when sharing. Non-personal information can be shared. Although we must be aware that if several sets of depersonalised data were merged or compared to each-other, there is a risk that an individual could be identified and this would also be deemed as personalised information.

For personal and sensitive personal information certain rules apply when sharing information.

The chart below shows the steps that will be taken when deciding whether or not to share information.

Sharing Information – Decision Making Chart



Is the information 'personal'?

Personal information is information which relates to a living individual who can be identified from that data. For example, data identifying the name of a family member, or their address.

Is the information 'sensitive'?

According to the DPA 1998, sensitive personal data means personal data consisting of information as to -

(a) The racial or ethnic origin of the data subject,
(b) His[Her] political opinions,
(c) His[Her] religious beliefs or other beliefs of a similar nature,
(d) Whether he/[she] is a member of a trade union
(e) His[Her] physical or mental health or condition
(f) His[Her] sexual life,
(g) The commission or alleged commission by him/[her] of any offence, or
(h) Any proceedings for any offence committed or alleged to have been committed by him/[her], the disposal of such proceedings or the sentence of any court in such proceedings.

The threshold for sharing sensitive information is generally higher than for sharing other personal information. This is because the unnecessary or inappropriate sharing of this sort of information is more likely to cause damage, distress or embarrassment to the individual(s) concerned.

It is the responsibility of the agency who owns the information about a family or individual to decide on a case-by-case basis whether there is a need for other practitioners to be made aware of any personal and/or sensitive information. If it is considered that there is a need to share this information, explicit consent **must** be sought from the individual who it concerns.

The information **cannot** be shared without the individual's consent for the sharing of this particular sensitive personal information, unless one of the following conditions under Schedule 3 of the DPA 1998 applies:

- Processing is required to comply with employment legislation.
- Processing is necessary to safeguard the vital interests* of the data subject or another person.
- The information has already been made public by the data subject.
- Processing is necessary in connection with legal proceedings.
- Processing is necessary for the administration of justice.
- Processing is necessary for medical reasons.
- Processing is necessary for ethnic monitoring.

* 'vital interests' of the data subject or another person refers to life or death situations.

Obtaining explicit consent and definition of a 'family'

Consent is a legal requirement for services not considered to be under Section 47 of the Children Act 1989.

Consent to share information and data should be gained for every adult family member aged 16 and over and by the parents/carer for children under the age of 16.

However, by definition, families engaging with services may be chaotic, unstable and in a state of flux. A professional judgement will be made in conjunction with the referring agency as to the composition of the family from whom explicit consent will be sought. This will need to be kept under review. If, at subsequent professionals' meetings it is considered that the care planning process would benefit from the engagement of a further family member, specific consent will need to be sought.

Consent must be a specific, informed and freely given agreement. In obtaining consent, each individual must be made aware of:

- Why we want the information.
- How it will be used.
- Who it will be shared with.
- The consequences of giving consent.
- The consequences of withholding or withdrawing consent.

Consent of the family is sought after referral and **prior** to the engagement of the family.

A specific Consent Form may be used for this process.

Consent withdrawal

Consent can be withdrawn by the family/family member at any time. Family members will be made aware that they have the right to do this. However, they will also be made aware this will have consequences for the engagement of that family in services which rely on inter-agency information sharing.

If consent is withdrawn, but it is considered that a statutory exemption applies concerning that family and/or family member, then it may be appropriate for professionals to share relevant information on the need to know basis.

Capacity to provide consent

All people over the age of 16 are presumed, in law, to have the capacity to give or withhold their consent to sharing of confidential information unless there is evidence to the contrary. The *Mental Capacity Act 2005 Code of Practice* will be followed when it is considered by relevant professional that a family member does not have the capacity to make decisions.

How to decide whether or not there is a ‘need for another professional to know’

Need to know within the context of service provision is determined on a case-by-case basis. Need to know is determined by assessing whether the sharing of the information with another professional in the Team (or other professionals from different agencies) will have an impact on the level and type of support and intervention that can be used for the family.

Need to know for the purposes of delivering a service means that the sharing of personalised information will likely be restricted to the individuals that assess the families, deliver the care package, and track the case progression.

If, after a care plan has been devised and is being implemented, it is felt that the services of a particular professional will not be required for the delivery or tracking of the case plan, then that professional does not have a need to know the personal information of that family.

Conversely, if the Care Plan is modified and new or additional professionals are required in order to deliver it, then these professionals have a need to know the personal information of this family.

How to decide to ‘Protect People from harm’

This is determined on a case-by-case basis.

Consider:

- Is there evidence that a person is suffering or is at risk of suffering significant harm?
- Is there reason to believe that a person is suffering or is at risk of suffering significant harm?
- Will sharing the information prevent significant harm arising for that person?
- Will sharing the information prevent other people or the public from experiencing harm?

There are no absolute criteria on which to rely when judging what constitutes significant harm. Sometimes, a single traumatic event may constitute significant harm, for instance a violent assault. More often, significant harm is a compilation of significant events, both acute and long-standing, which interrupt, change or damage a person’s physical and psychological development. Harm does include impairment suffered from seeing or hearing the ill-treatment of another.

To understand and establish significant harm for a child, it is necessary to consider:

- The family context;
- The child's development within the context of their family and wider social and cultural environment;
- Any special needs, such as a medical condition, communication difficulty or disability that may affect the child's development and care within the family;
- The nature of harm, in terms of ill-treatment or failure to provide adequate care;

- The impact on the child's health and development; and
- The adequacy of parental care.

The key factor in deciding whether or not to share personal and/or sensitive information where consent has not been sought is proportionality. In making the decision you must weigh up the risk of what might happen if the information is shared against what might happen if it is not. Consider the interests of protecting people against the interest in maintaining public confidence in the confidentiality of public services, an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals.

How to decide to 'Prevent crime and disorder'

This is determined on a case-by-case basis.

Consider:

- Will sharing the information prevent crime and disorder?
- Will sharing the information assist in detection or prosecution of crime and disorder?
- Is the intended disclosure of information proportionate to the intended aim?

The key factor in deciding whether or not to share personal information where consent has not been sought is proportionality.

Is sharing the information a proportionate response to the need to protect the public interest in question?

Proportionality is one of the key factors in deciding whether or not to share confidential information without consent i.e. when disclosing information without consent one must limit the extent of the disclosure to that which is absolutely necessary to achieve the aim of disclosure (e.g. child protection).

In making the decision you must weigh up the risk of what might happen if the information is shared against what might happen if it is not. Consider the interests of e.g. preventing crime and disorder against the interest in maintaining public confidence in the confidentiality of public services, an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals.

Secure transfer of confidential documents

All personal information shared must be both stored and disseminated in a secure manner.

- Internal email systems are considered secure, e.g. an email from one bexley.gov.uk account to another should be considered safe. All documents should be denoted as 'Confidential' where they contain personal or other data. Emails can be changed to 'Sensitivity/Confidential' through Outlook settings.

- Secure email. Many 'normal' email accounts (e.g. .gov.uk, nhs.uk) are **not** secure and should **not** be used for the transmission of any personal and/or sensitive information. All personal information must only be emailed using a secure email address that is featured in the listing below:
    - *.nhs.net (NHSmail)
    - *.gsi.gov.uk
    - *.gse.gov.uk
    - *.gsx.gov.uk
    - *.mod.uk
    - *.police.uk
    - *.pnn.police.uk
    - *.scn.gov.uk
    - *.cjsm.net
    - *.gcsx.gov.uk

- All Local Authority staff who are set up with a GCSX account must use this as their default email option for confidential material, when communicating with other Government bodies. GCSX mail forms part of the Public Services Network (PSN) which is the collective term used for the various Government networks that are all connected together. As a result GCSX mail can be used to securely share data between local authorities, central government departments and other organisations that connect to the PSN such as the Police and NHS. Note, however, that it is **not possible** to send email from a secure (GCSX) domain to an insecure one, only from secure to secure, ie a message cannot be sent to a bexley.gov. address from GCSX or vice versa, but can go to .nhs.net or .pnn.

- Egress Switch system – this is a web based secure email system which can be used by most organisations and is the LB Bexley default system for secure communications with schools, the voluntary and community sector, or non-public sector organisations and individuals. It involves mail recipients setting up a password protected account to access the secure document. It can be built in to Outlook for LBB staff at a small cost to the department.

  However**, Egress Switch will not work properly with health .nhs.net or police .pnn accounts**, and other means of transferring documents securely should be used.

  Website: https://switch.egress.com/ui/signin.aspx?ReturnUrl=%2fui%2fadmin

- Password protected document files. Word, .pdf and other file types can be password protected and sent through non secure systems. However, to follow Caldicott guidance,

passwords should not be sent using the same medium as the document, because if a digital intruder can access one email, they can access them all. For example, if you sent a passworded file by non-secure email, phone or text the password to the recipient. Passwords should follow good practice by being strong and hard to guess.

- By meeting - Through a recognised case management meeting (e.g. multi-agency meetings). Case management meetings should be closed meetings, only attended by the relevant managers, or other people who have been invited to attend in relation to a specific case.

- By hand - Personal identifiable information should only be taken off-site when absolutely necessary. Information must always be transported in a protected format. Personal identifiable information must never be left unattended and should be returned on-site as soon as possible.

- By secure mail (external) – This method should not be the default method to transmit information. However, there may be instances where this is necessary. If disseminated by external mail, information must be in a sealed double envelope, with full address and return address on the outer envelope, without the level of data or protective marking shown, and should be sent by recorded delivery.

Transmission by facsimile (fax) is **not** acceptable for personal information as it is not secure. This includes faxes sent between internal phone numbers. If faxing is necessary in **unavoidable** circumstances, safe haven principles should apply:

- Confirm the receiving fax machine is in a secure location
- Confirm the correct fax number is being used
- Confirm the named recipient is ready to receive the information
- Confirm safe receipt personally

Information Storage

Personal information shared must be stored securely at all times.

Agencies may need to store information relating to the work they are doing and the interventions they are delivering onto their 'home' case management system. In these cases care must be taken to only include information relating to that agencies' involvement and to avoid any inadvertent sharing of information beyond the need to know basis required.

No personal or sensitive information is to be stored on the hard drives of laptops or desktop computers. Only networked drives should to be used for this purpose.

No personal or sensitive information should be stored on any **unencrypted portable media** (e.g. CD/DVD ROM, USB Drive/'stick' etc.). Encrypted memory sticks should only be used where provided by the organisation's IT section.

Information in paper format should always be stored in a locked cupboard in a secure environment when not being actively used. Secure cabinets of the necessary specification will be made available for this purpose.

Information accuracy responsibilities

All agencies are responsible for ensuring that the information they supply is reliable by checking the quality of the information before they share it. In addition each agency is responsible for ensuring that inaccuracies in the information provided are rectified as soon as possible and before it is shared with the receiving parties.

Each agency is responsible for up-dating the information they share to ensure that the personal information remains correct.

Unresolved disagreements regarding the accuracy of the information between agencies should be documented by each member alongside the information that the disagreement pertains to.

Information Retention

Personal information should not be kept for longer than is necessary for its purpose(s).

Personal and confidential information will be retained in accordance with the relevant retention policy(ies) in place for agencies in Bexley (and which adhere to statutory requirements where they apply).

Information that is shared between agencies will be retained as agreed between agencies. These retention periods can be changed on a case by case basis if agreed by the originating agency. Considerations for judging retention periods include:
The current and future value of the information for the purpose for which it is held.

- The costs, risks and liabilities associated with retaining the information.
- The ease or difficulty of making sure the information remains accurate and up to date.

If a party is deemed not to be relevant to the delivery of the intervention package when the intervention package is devised, they will not retain the personal information received from other parties nor the collation of their own information.

Information should be disposed of appropriately and securely at the end of the retention period and in accordance with that organisation’s disposal policies.

Information Disposal

Personal and sensitive information must be securely disposed of. If it is in an electronic format, documents should be fully deleted from the computer system on which it is saved. If it is a paper document, it should be placed in a confidential bin for shredding.

Confidentiality agreement

A confidentiality agreement should be used at all meetings where personal information about a subject is to be shared amongst professionals attending that meeting.

Access and Individuals' Rights - Subject Access Request

The Data Protection Act 1998 gives individuals certain rights over their personal data. These include:

- The right to access personal data held about them,
- The right to know how their data is being used.
- The right to object to the way their data is being used.

Law and the Data Protection Act

Each partner working with children and families in Bexley shall comply with all of its obligations under law and the Data Protection Act 1998 and any subsequent statutes, orders or regulations in relation to its obligation under this agreement.

Information Sharing Agreements

A number of specific information and data sharing agreements exist in Bexley for specific purposes. These include:

MASH - Multi-Agency Safeguarding Hub

MARAC – Multi Agency Risk Assessment Conference

MAPPA – Multi Agency Public Protection Assessment