

Data Sharing Review

NSPCC response to a consultation paper on the use and sharing of personal information in the public and private sectors

Introduction

The National Society for the Prevention of Cruelty to Children (NSPCC) is the UK's leading charity specialising in child protection and the prevention of cruelty to children. The NSPCC aims to end cruelty to children by seeking to influence legislation, policy, practice, attitudes and behaviours for the benefit of children and young people. This is achieved through a combination of service provision, lobbying, campaigning and public education.

The NSPCC purpose is to end cruelty to children. In order to achieve this, it is vital that all children, whatever their needs, have a range of services that are flexible and offer them support and protection. The NSPCC has more than 180 services in the UK and the Channel Islands. These services aim to:

- Prevent children being abused by working with parents and carers in vulnerable families to improve their knowledge and skills in safeguarding, and giving children and young people someone to turn to through the provision of our Listening Services.
- Protect vulnerable children and young people from abuse by providing direct services in a number of settings, including schools and young people's centres. We also protect them by providing Listening Services for adults to ensure they have someone to turn to with their concerns; by ensuring that abused children and young people are identified and effective action is taken to protect them, and by working with young people and adults who pose a risk to children and young people to reduce the risk of abuse.
- Help children and young people who have been abused overcome the effects of abuse and achieve their potential. In drafting this response, we have drawn on what children and young people who use our services tell us about their experiences. We have also consulted a wide cross-section of frontline practitioners and service delivery managers who work directly with children and young people.

Section 1: Background

Question 1

The NSPCC welcomes the opportunity to respond to this consultation on information sharing. We undertake a range of activities focussed on ending cruelty to children and we are actively engaged in working to protect children.

Keeping children safe from harm requires professionals and others to share information and therefore this is a pertinent issue for the NSPCC.

The NSPCC considers that effective information sharing is an important part of delivering effective services to children and young people. It is essential to protect and safeguard them and to promote their welfare. However, sharing information without clear purpose and without clear authority is not likely to result in better services. There are risks of information overload and of sharing information which does not need to be shared. We consider that information needs to be shared intelligently. The lessons of the Victoria Climbié enquiry are not that information was not shared because of legal constraints but rather that information was shared in a chaotic and unfocused way, resulting in miscommunications and misunderstandings. Practitioners failed to act on information that was in their possession. That is a message that is repeatedly reinforced in Serious Case Reviews.

The NSPCC considers that keeping children safe from harm requires professionals and others to share information. However there is a need to balance that requirement with the need for children and young people to share confidences whilst retaining a measure of control over how sensitive information is processed and shared.

As a child protection agency, the NSPCC's order of priorities in regard to confidentiality and information sharing is:

- the welfare of children and young people is paramount
- respect for the principle of appropriate control by children and young people over the information they provide
- commitment to the concept that child protection is best achieved by a multi – agency approach described in '*Working Together to Safeguard Children*'.

The NSPCC keeps case-records for all work in which we are engaged and this information is retained in accordance with our retention schedule. The NSPCC holds this information on a central computer system (although historically these files were manual paper files). The NSPCC obtains this personal data from a variety of sources including the data subjects themselves and other third parties such as family members, carers, victims, statutory and voluntary agencies. The NSPCC shares information with appropriate agencies where this is relevant to safe-guarding or required by law.

The NSPCC's Services for Children and Young People also includes the NSPCC's 'Listening Services' which includes There4me; Childline and the National Child Protection Helpline. There4Me is an online interactive service that gives young people anonymous and confidential access to social workers. Our interaction with young people who access this service is

recorded, although this is not usually “personal data” as we are not provided with identifying information. As we are unable to identify the young person only limited information is shared with other agencies. However, young people are made aware at the outset that if they identify themselves to us and provide information that suggests that they are at risk of harm we have a responsibility to pass this information on to other organisations such as social services or the police. Childline is a confidential telephone service where trained volunteer counsellors provide comfort and advice to the 4,000 children who call each day. The NSPCC retains a record of these calls, although again this is often not “personal data” as less than 2% of callers provide identifying details. This information will not be shared with other agencies without the caller’s consent unless there is an immediate risk of the caller suffering significant harm. The National Child Protection Helpline is primarily for adults who need advice or who have concerns about a child’s welfare. All calls to the Helpline are confidential, except in a situation where a child is at risk and can be identified by the information given. About 28% of calls relating to the welfare of a child involved children at serious risk of harm, and resulted in referrals to the appropriate child protection agencies for further investigation.

Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

Question 2

Information sharing is a key child protection principle and is necessary in a number of contexts including in investigating child abuse, child protection case conferences, strategy meetings and serious case reviews. The appropriate sharing of information is vital to safeguarding children as it avoids the knowledge gaps that could result in a child being unprotected and enables agencies to target their response appropriately. The sharing of information is therefore beneficial to the individual child who can be protected, and to society who has a stake in ensuring that children are not harmed.

The sharing of information between professionals can also benefit a service-user as it can improve the support that they receive. Firstly, through sharing information it is possible to engage other organisations who can provide additional services of benefit to the service user. Secondly, if other agencies have similar concerns this can be useful in demonstrating to an individual/organisation that there are legitimate concerns that need addressing.

Finally, sharing information between NSPCC departments (with appropriate consent and due regard for the DPA) can also benefit individuals and society as it provides the information necessary for raising public awareness and influencing policy.

Question 3

The NSPCC acknowledges that keeping children safe from harm requires professionals and others to share information. However, there is a need to balance that principle with the need for children and young people to share confidences whilst retaining a measure of control over how their sensitive personal information is processed and shared. Children and young people need to be provided with a confidential space in which they can discuss openly issues pertinent to them. If too much information is shared, or if it is shared at too low a threshold, this could deter individuals in need from accessing or fully utilising the professional help available to them. For example, we know that young people feel more able to speak to Childline because of our policy of only sharing information at the serious and immediate harm threshold. Similarly, because young people can access There4me anonymously, this encourages young people to use the service.

As well as issues around whether information should be shared in the first place, there are also risks in relation to how information is shared. While technological advances have facilitated information sharing it is important that security concerns are adequately appreciated and addressed. There have recently been a number of high-profile security breaches in relation to personal data, which has served to highlight just how important this issue is. If information is not shared securely this can not only have a detrimental impact on the individual affected, but also on society whose trust is lost. This point is outlined in more detail in our response to question 20.

Question 4

Most methods and scope of information sharing pose both benefits and risks and therefore a balancing exercise must be performed. For example, technological advances have made information sharing quicker and easier, but this has created new security risks.

The sharing of information in child protection conferences or strategy meetings is an example of one method of beneficial sharing of information. It enables organisations to obtain a fuller more accurate picture and put issues in context, this in turn leads to more informed and appropriate child protection decisions being made. Similarly, the sharing of information is vital to serious case reviews. There is an inherent need for agencies to be open and honest during this review process so that lessons can be learnt. However, careful consideration needs to be given to how such information is shared more widely. Too much sharing could result in professionals being less candid and open which would undermine the purpose of undertaking such reviews.

One new method of information sharing that creates potential opportunities and risks is Contact Point, which operates in England. The NSPCC hope that Contact Point will be an effective way of flagging agency involvement and will help facilitate appropriate information sharing. However, there are risks associated with developing a large central database. The security of Contact Point is an obvious concern, although as security was an integral consideration during the development of Contact Point this will hopefully have resulted in a more secure system. Large government databases and the pulling together of different government departments under one umbrella, for

example the proposal that Contact Point, E-CAF and other e-initiatives are all under one umbrella, creates the risk of 'function creep'. It is important that effective safeguards and control measures are put in place to prevent this from occurring.

Question 5

Front-line child protection agencies tend to adopt a thorough approach to recording their involvement. While to some extent this may be justified by the need to be accountable for actions taken and to help ensure the quality of the service delivered, careful consideration must be given to whether this is beneficial to young people, especially if it deters people in need from seeking help.

The NSPCC has recently been concerned about the routine collection of Biometric data in schools without the necessary safeguards and protections in place. There are legitimate concerns about data security and if such data is used then robust procedures for maintaining confidentiality and data control must be established. Recent research carried out by the NSPCC has found that children themselves express considerable anxiety about the security of normal data that is held about them.

Question 6

The NSPCC has some concerns about the ways in which children's data is collected and used by private companies and the lack of transparency in relation to this. One aspect of this is in relation to the ways that marketing and advertising has followed children online. Recent research by Childnet and the National Consumer Council (NCC) 'Fair Game? Assessing commercial activity on children's favourite websites and online environments' found that in the commercial environment online data protection, fair trade and advertising rules are commonly flouted. Often parents and children do not read or understand privacy policies or take on board the way their data may be used by commercial companies.

Question 7

There exists confusion and inconsistency in relation to information sharing between the public sector and the voluntary sector in situations where voluntary organisations are performing activities usually undertaken by the public sector (either where commissioned by a local authority or undertaken independently of public bodies). This has resulted in information not being shared where it would be appropriate and beneficial to do so. For example, the NSPCC when commissioned by Youth Offending Teams to undertake assessments of young people who have received 'final warnings' or 'referral', 'supervision' or 'detention and training' orders for sexually harmful behaviour have been unable to obtain prosecution evidence to inform this work. While the NSPCC recognise the sensitivity of such information and the need to ensure it is not shared too readily, good practice guidance issued by the

Youth Justice Board recommend that this information is necessary to these assessments. Despite this the CPS have felt unable to share this information with the NSPCC on grounds that unlike the YOT with whom they could share this information, the NSPCC did not have a statutory duty to undertake this work. Similarly, the NSPCC's Specialist Investigation Service have encountered problems in obtaining necessary information from local authorities who have commissioned the investigation on the basis that this is prohibited by the DPA and notwithstanding NSPCCs authorised status under the Children Act 1989 and Children (NI) Order 1995.

Although legislation such as the DPA is often cited as the reason why information cannot be shared, such decisions can be based on a misunderstanding or misinterpretation of the DPA. It is the NSPCC's view that the real barrier to information sharing is often cultural or institutional barriers. Please see our response to question 11 for further detail.

It is the NSPCC's view that there needs to be an improved system of sharing criminal records between EU Member States to prevent sex offenders moving between states and gaining employment with children. The NSPCC has recently produced a report which makes a series of recommendations in relation to improving the exchange of information for the purposes of recruitment.¹ It shows that different countries in Europe will retain data about an individual's criminal convictions in different ways and for different lengths of time. There is also a lack of consensus between European countries about the appropriateness of sharing information for the purpose of vetting and barring and considerable complexity and variation in the processes for doing so. In our report we recommend that the European Commission produce a Green Paper on EU cooperation to monitor and exchange information about known sex offenders with the aim of preventing further abuse and actively take a role in promoting the exchange of experience and best practice between member states.²

Question 8

The disclosure of confidential counselling records in court proceedings is an area of concern for the NSPCC. The NSPCC provides therapeutic services to young people who have been subjected to physical or sexual abuse and considers the provision of such services to be important and beneficial to individuals and society in general. Legal proceedings are frequently not envisaged when such work is undertaken. It is only later that these young people become embroiled in criminal or contact/residence and care proceedings and the court orders the disclosure of NSPCC files, sometimes in

¹ Fitch, K with Spencer-Chapman, K. & Hilton, Z. (2007) 'Protecting children from Sexual Abuse in Europe: Safer recruitment of workers in a border free Europe', NSPCC: London

² Such standards and principles could include, for example, an agreed list of sectors and/or professions where vetting of individuals is compulsory, the frequency of checks, and mechanisms of redress for individuals.

a very general fishing exercise. It is the NSPCC's view that it is not in the public interest for these records to be disclosed to the defence in criminal proceedings or to the parties in family proceedings as this undermines the effectiveness of therapeutic services and can cause distress to the young person. In addition, valuable NSPCC resources are used in contesting the disclosure of this information at public interest immunity hearings. These sorts of applications for disclosure appear to be becoming more commonplace and erode the whole concept of confidentiality of personal information.

Another example of inappropriate data sharing is in a domestic violence context. Inappropriate sharing in these circumstances can compromise the safety of the children and/or the partner who is/was subjected to violence. It is important that appropriate consideration is given to the shielding of databases.

Section 3: The Legal Framework

Question 9

The DPA is important and coherent legislation that is vital to promoting and protecting an individual's privacy. The DPA provides a useful standard in relation to all processing of personal data to which data controllers must adhere. The DPA encourages all organisations to consider why and how they process personal data (in particular sensitive personal data) and to take adequate steps to protect the integrity and security of the data it processes. In general the provisions of the DPA work well and should not prevent or obstruct legitimate processing of personal data. It is the NSPCC's view that the main weakness of the DPA is not actually the legislation itself, but rather misunderstanding and misinterpretation (sometimes deliberate) of the requirements of the DPA. See our response to question 11 for further consideration of this point.

However, there are occasions where the Data Protection Act creates genuine difficulty for voluntary organisations undertaking work that could be considered to be a public function. While on occasion problems in relation to data sharing are avoided by virtue of the NSPCC being a data processor, this is not usually the case. Accordingly, the NSPCC will usually be the data controller and must satisfy a Schedule 3 condition as much of our work involves processing sensitive personal data. This creates difficulty not only for the NSPCC in sharing information with other agencies (see our response to question 16 in relation to JARs) but also in relation to information being shared with the NSPCC. Further guidance would be helpful in clarifying what Schedule 3 conditions are available to voluntary organisations that are undertaking functions that are conferred on public bodies by enactment or could generally be considered to be a public function in the public interest. A Schedule 3 condition in similar terms to Schedule 2, paragraph 5(d) could resolve some of the difficulties encountered.

Question 10

It is likely that the 2nd principle is adhered to by child protection agencies as far as understanding and interpretation allows. While the 2nd principle should be an important provision in preventing data sharing for incompatible purposes, there are situations where it is ambiguous as to whether a purpose is compatible or not and it is this which creates difficulty in adherence to the 2nd principle. Where it is obvious that a further purpose for processing is incompatible it is likely that organisations do adhere to the 2nd principle. For example, the NSPCC has implemented internal policies and procedures to ensure that consent is always obtained where we wish to use a service-users personal data for a purpose that could be considered to be incompatible. The Department for Constitutional Affairs has expressed the view that the “requirement of compatibility does not mean ‘identical to’ and provided the further processing is for a purpose not contradictory to the original purpose, it will be consistent with the second principle” (Data Sharing – Frequently Asked Questions <http://www.foi.gov.uk/sharing/faqs.htm> - accessed 18/06/2007). Nevertheless, the 2nd principle is at times interpreted to mean an identical purpose and this can lead to information not being shared where it is appropriate to do so. Conversely, what is or is not compatible can be interpreted widely which can lead to inappropriate data sharing. It is the NSPCC’s view that further guidance on the 2nd principle and the meaning of compatibility would be useful in promoting adherence.

Question 11

It is the NSPCC’s view that the greatest barrier to the effectiveness of the DPA is a lack of understanding or misinterpretation (sometimes deliberate) of the DPA’s provisions. The DPA is not always recognised as legislation that protects an individual’s privacy and instead can be perceived in more negative terms. Lack of understanding or negative perceptions of the DPA can on occasion result in a failure to share important information for fear that this might contravene the DPA. It is the NSPCC’s view that further guidance on data sharing, particularly sharing between the public sector and the private sector would be useful in aiding understanding of the DPA and overcoming the barriers that exist. In addition it would be helpful if there was an arbitrator who could provide definitive advice in relation to specific data sharing issues.

Question 12

It is the NSPCC’s view that a tougher stance needs to be taken in relation to data security breaches, particularly where this involves children’s personal data. Civil sanctions for failing to implement adequate security measures and greater powers of scrutiny for the Information Commissioner would encourage data controllers to take data security seriously and to put in place appropriate safeguards to prevent the loss and accidental disclosure of personal data.

In relation to whether data should be shared or not it is the NSPCC’s view that the emphasis should be on the provision of further guidance on when information can be shared, rather than sanctions as it is important that

practitioners feel able to share information where there are child protection concerns. If practitioners were fearful of sharing information, this might result in information not being shared where this is necessary to protect a child from harm.

Question 13

The common law of confidentiality and human rights legislation impacts on the DPA and data sharing and there is some confusion about how these sit together and inter-relate. For example, how do these laws inter-relate when confidential counselling information is requested by another organisation in relation to child care law?

Question 14

It may be useful if there were links to identification protocols as per Contact Point to ensure information is reaching the appropriate\correct person

Section 4: Consent and transparency

Question 15

While the NSPCC acknowledges the importance and merit of subject access rights, responding to a request can be very resource intensive and costly. This is particularly the case where the subject access request is made by an individual with a grudge against an organisation, or where it used as a means of achieving advance disclosure in legal proceedings. While a data controller does not have to comply with a request where to do so would involve “disproportionate effort”, this does not apply in relation to locating and sifting through information, which is often the time consuming and costly aspect to complying with requests. For example, if a former employee requests personal data held electronically, a computer search will generate a massive quantity of data. While most of this data will not be the individual’s personal data it is still necessary to sift through this information to locate the personal data. Although requests can be made to applicants to narrow their request, this does not necessarily speed up the process, nor is their assistance always forthcoming. It is the NSPCC’s view that there should be a disproportionate effort test in relation to sifting through information and/or a positive requirement on the requester to narrow the search terms if necessary.

Question 16

The form consent should take:

The DPA is clear that consent must be freely given, fully informed and specific to the circumstances. However, the difference between consent in Schedule 2 and explicit consent in Schedule 3 is not clear. It is widely considered that the main difference is that explicit consent requires the consent to be evidenced in writing, although this point does not appear to have been definitively confirmed.

When is consent required?

As regard whether it is clear when an individual's consent is required, it is the NSPCC's view that not all organisations or individuals are clear when consent is required. There is a common misunderstanding that consent is the only basis upon which information can be shared. Consequently, on occasion consent has been sought in situations where this would compromise a child protection investigation.

It can also be confusing as to when a child's consent is required if the parents have given their consent to information sharing. The NSPCC has adopted the approach that where a young person is '*Gillick competent*' their consent should be obtained. The NSPCC's Core Standards, Principles and Procedures to which SCYP adhere, provides guidelines on making this assessment.

Difficulties can also arise for voluntary organisations in establishing whether consent is required, where the sharing of information is required by other legislation, but it is ambiguous as to whether an organisation such as the NSPCC is subject to the other legislation. An example of this is Joint Area Reviews which were introduced by the Children's Act 2004 to monitor the standard of service being delivered to young people. It is not clear whether the NSPCC is actually subject to this legislation but our files have still been requested for inspection by the Joint Area Review board. If we are subject to the legislation then we would not need consent to share this information, but if we are not subject to this legislation then it is likely that explicit consent will be required as these files contain sensitive personal data.

NSPCC work involving consent:

While other conditions may permit sharing, in appropriate circumstances the NSPCC considers it to be good practice to obtain a service-users consent and therefore the NSPCC does attempt to engage an individual in the decision to share their personal data. In addition, at the outset of work with an individual service-user the NSPCC provides an explanation of how we will be processing their personal data and our duty to share information with appropriate agencies where there are child protection concerns. The NSPCC also attempts to engage even young children by providing this information in simple language that can be understood by a child. The NSPCC has developed templates and procedures for NSPCC practitioners to use and follow when obtaining this consent from service-users.

The NSPCC may also request consent even when an exemption from the non-disclosure provisions might apply. For example, where the police request access to NSPCC records we may require the consent of the data subject before we release any information, even if section 29 DPA is satisfied. However, there can be difficulties in assessing whether the consent the police provide is informed consent as we are no longer working with the data subject and therefore we cannot assess whether the individuals understands the repercussions i.e. this information may be disclosed to the defence, or their capacity to give consent.

Question 17

As outlined in question 16 the NSPCC considers it to be good practice to engage a service-user in decisions in relation to sharing their personal data. However, there are occasions where a requirement to obtain consent would prejudice the work being undertaken. For example, our Specialist Investigation Teams need to be able to share information with other agencies such as social services and police where during the course of their investigation they uncover information that raises serious child protection concerns. In these circumstances it is unlikely that consent would be forthcoming, it might also be prejudicial to inform the individual that we would be passing information to the police.

Question 18

It is the NSPCC's view that data subjects already have considerable rights of access to their personal data and that these do not need of strengthening. In the NSPCC's experience a data subject usually request access to their entire file and not extracts of it. In such circumstances the data subject obtains a complete picture of what personal data an organisation is holding and how it has been processed, including who it has been disclosed to.

It is the NSPCC's view that organisations should be encouraged to be open and transparent and engage individuals in decisions to share their personal data. However, it is important to ensure that organisations understand the exemptions from the subject information provisions where informing individuals about the sharing of their personal data would prejudice child protection work.

Question 19

The NSPCC believe that many organisations in the voluntary sector already strive for transparency in relation to the records that they hold on their service-users. To some extent transparency, scrutiny and accountability is already provided for by the access rights enshrined in the DPA. The NSPCC considers the Framework code of Practice for Sharing Personal Information to be useful, particularly for those organisations with limited expertise in the area of data protection. However, more detailed technical specialist guidance is required. The Department for Constitutional Affairs' 2003 guidance on public sector data sharing is extremely useful and it would be helpful if it could be broadened to cover data sharing between the public sector and voluntary organisations delivering similar services.

Question 20

Technological advances have increased the ease and speed of sharing information but as well as creating benefits this has also created new risks. The positive impact of technological advances is that it is possible to obtain or share information more quickly. If used properly this can improve the way in which services are planned and distributed and can result in earlier

intervention which can reduce or eradicate the harm suffered by a young person. Improvements in technology has also enabled the development of systems such as Contact Point which should be useful in facilitating joined up working between child protection agencies.

However, these technological developments have also created new security risks. Sensitive information or large quantities of information can now be downloaded on to small portable devices or emailed, which makes further dissemination much easier and greatly increases the risk of loss or accidental disclosure. The accidental loss or disclosure of sensitive personal data can not only cause immense damage or distress to the individual affected, but it is also damaging to society who loses trust in the organisations processing their personal data.

Another negative impact of technological advancements is that at times new technology has inappropriately changed practice rules. It is the NSPCC's view that technological advances should facilitate sharing and not dictate policy and practice. It is important that decision about how service-users personal data is processed is guided by practice and ethical issues rather than by what is technically possible.

Question 21

While the interpretation of Principle 7 is useful guidance, the NSPCC would welcome more specific guidance on technical safeguards that should be adopted to protect personal data. However, any standards that are developed must keep pace with technological advancements. There is a danger that if requirements are too prescriptive they would quickly become out of date.

Question 22

It is the NSPCC's view that anonymisation is a useful technique in safeguarding privacy. However, in the NSPCC's experience further guidance on how to do this effectively is required. It would be very useful if such guidance was available for free from the Information Commissioner's website.

Section 6: International Comparisons

The NSPCC only operates in the UK and Channel Islands and therefore we are unable to make international comparisons.

Section 7: Additional questions

Q27/28

Most of the guidance on data sharing centres on sharing between public authorities or between private bodies. There is very little guidance on the sharing of information between the public sector and the private/voluntary

sector who are delivering work of a public nature on behalf of a the public sector. Such guidance would be welcomed.