Information Commissioner's Office

Promoting public access to official information
and protecting your personal information

# Protecting Children's Personal Information
# ICO Issues Paper

## 1. Introduction

Never before has so much personal information been collected about children. And the volume is set to increase dramatically.

Information about children, and those associated with them, is collected for the best of motives. We all wish to protect children from abuse and other forms of harm. We all wish to see every child fulfil their potential with the best possible education, healthcare and social and emotional development. We all wish to stop children drifting into crime and anti-social behaviour.

There are – and always will be – fierce, and often emotional, controversies about how such lofty aspirations are to be achieved in practice. A particular focus is the role of official bodies concerned with the well-being of children. The ongoing debates about where and how to draw the boundary lines for state intervention must be largely resolved at political and democratic levels.

But initiatives within this broad field throw up real data protection and privacy issues which need to be addressed. The fact that data protection law (at European and domestic level) does not draw any explicit distinction between data subjects who are adults and those who are children introduces an important extra dimension that must also be addressed. Many of the issues about the handling of information about children are difficult and call for delicate judgements. The answers will depend on policy direction taking into account important data protection considerations.

This Issues Paper covers three main areas – facts, issues and future actions. The first area covered highlights the extent and range of personal information collected on children by official bodies, how this is (or will be) used and with whom it is shared. Many existing and proposed schemes will not be controversial, but the overall picture and the increasing links between the different schemes may surprise some people.

The paper then stands back to identify some of the key data protection issues and raise questions about them. Clarity about purposes, rationales and legal authority are important considerations in deciding what is acceptable and what is not. But there are other practical, and perhaps more pressing, matters which must be addressed if significant risks are to be avoided.

The final section sets out future directions which the Commissioner will be adopting. This includes immediate and prospective guidance on some matters (such as consent) and other more policy-based initiatives. A central theme is to help the various official bodies to get it right, not least to ensure maximum public trust and confidence in what they do. Our approach therefore is one of constructive engagement, not sceptical or negative confrontation.

This Issues Paper draws upon a research report prepared for the Information Commissioner's Office by the Foundation for Information Policy Research (FIPR). The research report is being published at the same time and examines many aspects in far more detail. The views and conclusions set out in the FIPR report are their own, not those of the Commissioner or his Office.

## 2. The growth in information held about children – the facts

The FIPR research provides a comprehensive account of the range of databases containing information about children in the areas of social services, education, youth offending and healthcare. It also examines the development of new core systems to aid information sharing such as the Information Sharing Index. The report identifies the stated public policy objectives underpinning each initiative, the range of personal information held and how this is used and disclosed in practice. It shows that increasingly the motivation for initiatives has moved on from concentrating on child *protection* to increased emphasis on child *welfare*, including such matters such as poor school performance and poverty. There are also moves to try to address matters that are of more relevance to the community at large. This includes collecting and analysing risk factors in order to try to identify those who may be involved in crime later on in life.

These are the major or innovative databases which collect (or soon will collect) information about children in England.

| Scheme | Used by | Contents |
|---|---|---|
| Information Sharing Index (IS).<br>To be introduced by 2008. | Dept. for Education and Skills (DfES) and Local Authorities (LAs) | Basic details identifying all children, with contact details of practitioners and indicators of concern. |
| | | |
| Integrated Children's System (ICS).<br>Proposed. | Social Services | "Electronic social care record" (ESCR) for children's cases being handled by social workers. Would store and analyse very full details on children and their families. Would download data from other databases but wouldn't |

| | | |
|---|---|---|
| | | automatically share data in return. |
| | | |
| National Pupil Database (NPD). | DfES | Extensive factual details of every child in state education in England. |
| | | |
| RAISEonline (Reporting and Analysis for Improvement through School self-Evaluation). To replace similar existing system. | Ofsted and schools | System for analysing the data in the NPD. |
| | | |
| “Lost pupil” databases | Local Education Authorities (LEAs) | Most recent NPD data for children not currently in state education in England. |
| | | |
| ASSET | Young Offenders’ Teams (YOTs), Youth Inclusion and Support Panels (YISPs) and youth courts | Profiles of young offenders, based on a variety of factors, for the purpose of sentencing and rehabilitation. |
| | | |
| ONSET<br>Currently at pilot stage. | YISPs. Funded by Youth Justice Board. | Same as Asset but for non-convicts. To identify those most likely to get into criminal behaviour. |
| | | |
| RYOGENS | Produced by Esprit and currently used by five LAs | Concerns about vulnerable children and young people. |
| | | |
| National Register of Unaccompanied Children (NRUC) | Promoted by Association of London Government. Used to exchange information between LAs and Immigration and Nationality Directorate (IND) | Exchanges information between IND and LAs about unaccompanied under-18 asylum seekers. To manage funding for the care of these people and to reduce the use of false ages by asylum seekers. |
| | | |
| NOTIFY | Greater London Authority and London boroughs. | Placement and movement of homeless households |
| | | |

| | | |
|---|---|---|
| MERLIN | Metropolitan Police | Children 'Coming to Notice' (CTN) of the police. |
| | | |

The **Information Sharing and Assessment Index (IS)** contains only the contact details for the child, their school, GP, and anybody else who is providing them with public services. No further information (such as health or education records) is included. If one person involved in the child's welfare wishes to speak to the others, they can put a flag on the record to ask others to contact them.

The database can be accessed by specific, vetted staff in a variety of agencies involved in child services. Where data is particularly sensitive – for example, a child has been seen by a mental health specialist – then access to this information is subject to further safeguards, and will be available only with explicit consent. Children's contact details will only be omitted from the register where there is a real risk that including them could put them in danger.

The **National Pupil Database** contains full details on all children in state education, including examination results, ethnic background, and whether they receive free school meals. **RAISEonline** will be used by the school inspections board Ofsted and by Local Education Authorities (LEAs) to analyse the data in the National Pupil Database. This can show up, for example, that a certain school needs to do more for children with special educational needs, or that children of a certain ethnic group are falling behind at school. It can also be used by individual schools to predict the results of their own pupils.

**RYOGENS** is a system used by health, social work and education officers within Local Authorities to record general concerns about a child's welfare, such as involvement in bullying, or the fact that a child lives in a disadvantaged area. If a certain number of concerns are registered, the system will automatically notify the other relevant departments within the same Local Authority. At the date of the FIPR research for their report it was only being used by five Local Authorities.

**Notify** is used by various local government authorities in London to keep track of the movements of families placed in temporary accommodation. Full health, housing and social services reports will be uploaded, but these types of data are available only to professionals dealing with that aspect of the family's care.

**MERLIN** is a Metropolitan Police system which records every child who has come into contact with the police in any way, whether as a victim, an offender, because they are living in the same household as an offender, or for any other reason.

The majority of these databases only allow access to information within the relevant sector, such as education or social care. The main exception is in systems which are designed to reduce youth crime and anti-social behaviour. RYOGENS, for example, allows non-consensual sharing of information between social services, police, health, education, housing and YOTs.

## 3. Issues and questions

There is a need for full debate about the range and extent of information being collected on the nation's children. It is hard to envisage any households with children remaining untouched by at least one of the various databases that are being compiled. Whilst these can serve essential public policy objectives, the collection and use of some information may be moving into areas which create a feeling of unease. The profiling of children at an early age from circumstantial matters and the consequences for the rest of their lives is a particular example.

This Issues Paper will be used to increase awareness of what is happening and will generate and structure further debate. Those most closely involved may wish to study the wider and deeper analysis offered by the FIPR report.

The Information Commissioner's position must be more closely tied to his data protection responsibilities, especially to consider a number of key data protection issues which are generated by the plethora of children's databases. They relate to both design and implementation and are expressed in general terms, but the Commissioner is aware that the promoters and practitioners for some schemes are addressing the various concerns more rigorously than others.

The main issues – broadly mapping on to the most relevant statutory data protection principles – fall within these headings:

- child protection as a priority;
- primary and secondary uses;
- fair and lawful processing;
- accuracy and quality of information;
- security;
- rights – especially access to records.

### Child protection as a priority

Protecting children from a real risk of harm from abuse or neglect, usually from their parent or carer, must always be a priority. It is widely accepted – legally and ethically - that confidentiality can be broken on pressing child-protection grounds. This has long been an integral part of the daily operations of social workers, doctors, teachers, the police, and those providing advice on information handling issues within these services. By sharing genuine

concerns about a child or family, professionals can construct a more accurate and comprehensive picture about a child's safety and well-being. Sharing information may be especially important, given the extreme lengths abusers may go to conceal their wrong-doing.

It is important to re-state that data protection law never stands in the way of using or sharing personal information – about the child and sometimes about others - where a real need exists. Harming children though abuse or neglect is criminal activity. Data protection law recognises the importance of preventing and detecting crime and pursuing offenders. This must be especially important where children are the victims.

Data protection should never be used as an excuse for failure to protect a child from a real risk of harm.

Data protection issues may be less clear-cut where the concerns focus on the welfare of children, rather than their protection. Child protection and child welfare are not the same thing. Child welfare is a much broader category - referring to children who are poor, or unhappy, or living in unsatisfactory neighbourhoods, or at risk in some other way of not growing up into happy adults with a reasonable chance to fulfil their potential. While child protection deals with a relatively small number of children – estimated to be around 50,000 in England - child welfare concerns may exist for three to four million.

The *Every Child Matters* agenda extends social care from protection to welfare. Although there are overlaps, this shift means that substantially more information will be collected and shared about substantially more children for different reasons. These different purposes raise different considerations from a data protection perspective. It is important that approaches used in the context of protection are not assumed to be transferable to the welfare context. The blurring of boundaries with the prevention of youth offending complicates matters still further.

**Primary and secondary uses**

Confusion or uncertainty about the protection / welfare boundary illustrates well the importance of ensuring clarity about the purposes for which information is collected and used. A fundamental and well-established data protection requirement is that personal information should be used for specified purposes and should not be processed in ways which are incompatible.

Those designing and using any scheme which collects and uses information about children must be absolutely clear about their purposes. There must be a degree of specificity and the boundaries of the purposes must be clear. Any secondary purpose needs to be clearly justified. These matters are particularly important where information is shared from one agency to another, especially from one discipline to another. It may be necessary to ask whether the law needs to be changed to allow broad data sharing in child-

welfare cases as well as child-protection cases. However, even if statutory gateways to information sharing are created, it is still important that there is clarity about which information should be used for what purpose. This needs to be reinforced by appropriate guidance and training for practitioners.

The FIPR report claims that some recent or prospective schemes provide examples of these concerns. The authors of that report were particularly concerned about the Connexions database, the purpose of which is defined in the Learning and Skills Act 2000 (s.114) as being to '*encourage, enable or assist … effective participation by young persons in education or training*'. However, data from this system can be passed on to other bodies involved in, for example, encouraging young people to stay out of crime. The report also highlighted the gradual shift in purpose of certain databases over time. The National Pupil Database was originally intended to contain only anonymous data for monitoring purposes, but it now contains data which can be used (via RAISEonline) to inform decisions about individual pupils. RYOGENS, initially justified as a crime prevention tool, is now used to share lower-level concerns on children. The result is that children and parents may not have a clear understanding of the scope of a project or how their data is likely to be used in the future.

**Fair and lawful processing**

The central thrust of the FIPR Report is that the collection and sharing of information about children may not be easy to justify as fair and lawful. In particular, the report focused on the question of whether a child may give consent for their data to be used without reference to their parents. The Information Commissioner recognises the difficulties involved in judging whether a child is capable of giving fully informed consent, and he would always recommend as good practice that parents should be consulted about important decisions affecting their children. Nevertheless, it must be emphasised that the Data Protection Act 1998 confers rights on the Data Subject, i.e. the child. These rights should only be exercised by another *on their behalf* if they are not capable of exercising them independently. Given the continued development of case law touching upon the autonomy of a child, the Commissioner believes that the time may be right for him to issue further guidance in the context of data protection rights and obligations. The ICO will be reviewing what it can do to provide a clearer steer for those having to deal with difficult practical decisions.

However, consent will not always be the only way to ensure fair and lawful processing. Indeed, given the difficult issues that have been mentioned, it may be safer for data controllers to rely on another basis for the processing. It is certainly not the intention of the Data Protection Act to deprive children of protection where parents unreasonably refuse their consent. It is also important that the seeking of consent is not undertaken on an inappropriate basis such as where processing is likely to go ahead with or without consent,

The authors of the FIPR report have also raised concerns about the legal bases for processing and the use of so-called “statutory gateways” as an alternative to consent where information needs to be shared. Statutory gateways can vary from the permissory in terms of providing legal powers through to ones based upon compulsion. The effects in data protection terms vary depending upon the approach adopted. Compulsion can override some aspects of the Data Protection Act whereas providing that information may be shared still requires substantial data protection compliance. Information sharing issues are already the subject of substantial work by Government and the ICO is also developing further practical guidance including a framework code of practice for information sharing to help practioners in a complex area.

**Accuracy and quality of information**

There can be no dispute about the importance of recorded information about children being accurate and up to date. It is almost incidental that these are legal requirements. No professional dealing with a child wishes to work with inaccurate or outdated information. A child or its family can be seriously damaged if inaccurate information is recorded.

Although this is not an aspect that was fully explored in the FIPR report, the growth of databases holding information about children increases the risks substantially. Collecting more information increases the potential for mistakes being made whilst entering (or failing to update) information and the wider use and sharing of it magnifies the potential effect of such mistakes. Other risks arise as one database shares information with another, especially where updates do not routinely follow initial data transfers. The fluidity of modern life, with frequent changes of address and family composition, exacerbates the problems further still.

The need for quality goes beyond the quality of the data itself. It also raises questions about the quality of the systems for structuring, accessing and searching for the information. In particular, if too much information becomes impenetrable, the risks of overlooking the really important indicators magnify - the “Needle in the haystack” problem.

Examples of the risks that can materialise include:

- mistaken identity;
- inaccurate, missing or out-dated information about the circumstances or characteristics of the child or family;
- inaccurate, missing or out-dated information about contact between professional and child;
- “missed alarms” (Climbié) and “false alarms” (Orkney) - poor data quality will simultaneously make both error rates worse;
- incorrect inferences drawn from ambiguous, incomplete or misleading information.

## Security

Any database containing personal details needs to be surrounded by appropriate security. The Data Protection Act requires that the level of security takes into account the harm that an individual may suffer as a result of a breach of security. The consequences of the most personal details of vulnerable members of society falling in to the wrong hands, such as those who may seek to prey on individual children, could be extremely serious.

The level of security will need to take account of such potential harm and be at an appropriately high level. This cannot be left to chance and needs designing into systems from first principles and reinforced by the systems of work surrounding their operation. Clearly establishing systems that are designed to be consulted by many individuals needs rigorous access controls. Similarly, the human element is particularly important where information may be shared between practioners not known to each other. It is essential that all the following areas are adequately addressed:

- physical security including the location of computer equipment and physical access to them, especially portable devices such as laptops;
- logical security including passwords and differential levels of access dependent upon user needs;
- management and technical procedures to ensure effective security and monitoring of access such as by the use of audit trails;
- staff training to ensure that information is not misused or wrongly disclosed to others backed up by appropriate disciplinary measure where staff knowingly contravene security procedures.

The Commissioner has already called for tougher penalties for those whom deliberately seek to misuse personal information and the potential of children's details falling into the hands of those who may do them harm underscores the need for effective criminal penalties to deter and punish.

## Rights of access

One of the key features of data protection legislation is the right of access provided to individuals. Some databases which may include predictive profiling and these and others may affect how an individual is treated by those that they come into contact with. It is essential that individuals can readily check the extent, nature and accuracy of the personal details held about them or their child where the child is incapable of exercising the rights for themselves.

It is essential that appropriate procedures are in place to ensure that this right of access is complied with within the statutory time period (40 days). Where children are involved judgements may have to be made whether the child is capable of exercising their rights for themselves or whether it is appropriate for a parent or guardian to do so on their behalf

## 4. ICO future actions

The Commissioner's immediate priority is to ensure that the issues raised in this paper reach a wide audience, including policy makers, the bodies collecting and using information on children and all who are concerned about how children's privacy rights are protected.

Various more specific directions can be identified:

### Guidance from the ICO

It is clear that policymakers and practitioners need and would welcome practical guidance from the Commissioner's office on issues relating to children's databases.

### Consent

Guidance on consent issues is a priority and a technical guidance note on this will be issued in due course. The ICO is also in the process of preparing a framework code of practice to assist public sector organisations in setting up information sharing schemes.

### Templates

The ICO will also explore the value producing easy to read guidance in a template format which can be used by social services to explain basic data protection matters to their clients This will be in a form of a template which will enable and encourage practitioners, possibly in partnership with others, to tailor the template so as to explain their own approach and deliver the guidance directly to affected families. It will include such matters as opt-out and access rights. There may be scope to adopt a similar approach to education and health professionals.

### Subject access requests

The ICO will consider whether further guidance on responding to subject access requests is needed to help organisations decide when it is appropriate to respond to a subject access made on behalf of a child, such as by their parent, and when a child must exercise the rights for themselves

### Young people

The ICO will consult relevant interests with the aim of drawing up a programme to prepare fresh guidance aimed specifically at young people, notably those in the 12-18 age range. This may be tackled both generally (all children) and selectively (eg those in contact with social services and/or police). All of it will reflect how children value their own privacy and confidentiality and help them to understand how they can best safeguard their own interests. The ICO is particularly concerned to work alongside bodies

such as the Children's Commissioners, who share a common interest in many of the issues set out in this paper.

**Constructive engagement with government and policy-makers**

In a spirit of constructive engagement, the Commissioner will be discussing issues relating to children's databases with government departments leading on education, health and youth offending. Particular priorities will include:

- Minimising the risks of profiling - where a child is placed in a risk category, it becomes very difficult for them to ever be viewed in any other way by those who come into contact with them in the future however they conduct themselves. This form of stigmatising runs the risk of becoming a self fulfilling prophecy for those affected.

- Ensuring that appropriate mechanisms are in place to reflect the views of parents and children when obtaining information including ensure that consent is sought where necessary and not used on a inappropriate basis.

- Establishing the most appropriate way to share information.

- Data quality.

- Security.

- Establishing the value of 'Privacy Impact Assessments'.

- ICO involvement in future policy development.