

Privacy Guide for Parents



Information about children is collected from the moment they are born. Some of this is necessary, some isn't - and some of it is gathered without your even being aware that it is happening. It is important that you know what data is being collected, what it's used for and how to keep as much control over it as possible.

[What sort of information?](#) In this pack you will find some examples of what we mean.

Kindly supported by



THE Joseph Rowntree
REFORM TRUST LTD

Bloodspots

What is it? Soon after birth, a tiny amount of blood is taken from a baby's heel and transferred to a 'Guthrie Card' as a series of small spots. These are used to carry out routine checks for any potentially serious health problems. You can get more information here:

<http://newbornbloodspot.screening.nhs.uk/FAQs#1c>

In England and Wales babies' blood spots are stored for a minimum of five years. Some hospitals keep them until adulthood.

Will you know it's happening? Yes, parents are asked for their consent to this procedure.

Pros and Cons: the tests are undoubtedly very important but once you have given consent to any of them, you have no further control over whether the bloodspots are used for other research, nor for how long the Guthrie Card is kept. This is in contrast to many other countries. In Scotland, for example, parents can specify that the Card is only kept for 12 months:

<http://tiny.cc/y7or0>

What you can do: If you believe that you should have the option of requesting destruction of the Card once tests are complete, talk to other parents in your area and consider making a joint approach to your MP to raise your concerns.

Bounty Packs

What are they? Bags containing free samples and leaflets that will be offered to you shortly after your baby's birth, in exchange for some personal details.

Pros and Cons: everyone likes getting freebies, but be aware that the information you give will be used to target marketing at you in the future. Bounty is described as: "*one of the largest advertising and communications companies in the world*" that "...*can use their 9.1 million strong database to gain useful data. 96% of parents give information about their family and lifestyles to Bounty and 80% of parents give permission for Bounty to pass their details to selected brands.*" For more information, see: <http://www.starmedical.co.uk/profile-bounty-uk.php>

What you can do: If the idea of having your information passed to a variety of companies concerns you, simply refuse to hand over your details.

Contactpoint

What is it? This is a new, national government database containing the contact details of every child from birth to 18 plus a list of every service that the child is using. It is designed to allow practitioners to contact each other directly to discuss your child. A central plank of the government's 'Every Child Matters' agenda, the idea behind Contactpoint is that all children can be monitored for signs of 'problems'. Despite the rhetoric, this is not a child protection system.

Will you know it's happening? No. Children are automatically entered on to the database at birth

Pros and Cons: It is difficult to find any benefits to this system, other than the convenience of practitioners, and both opposition parties have pledged to scrap it at the first opportunity. Around half a million people will have access to the Contactpoint system and although much has been made of its strong security features, it is impossible to make such a large-scale system secure. The potential to exclude parents from discussions about their own children's welfare is also extremely worrying, as is the possibility that families may start to avoid using the services that they need, once they realise that all access is logged on Contactpoint.

What you can do: Although you cannot stop your child's details being included, you may be able to get your child's record 'shielded' (hidden) on the system if you believe that unauthorised access may put you or your child in danger. If this is the case, you should contact your local authority at once. You should also keep an eye on the accuracy of the information by making regular Subject Access requests – this process is explained further down.

eCAF

What is it? This is another new, national database to complement Contactpoint, designed to store the personal profiles of children that are created under the 'Common Assessment Framework' (CAF). These assessments are for any child seeking services - the government estimates this is around one-third of the child population at any time. The information is available to any practitioner working with a child. A description of the CAF, including the type of assessments that a practitioner is asked to make, can be seen here:

<http://www.dcsf.gov.uk/everychildmatters/download/?id=1290>

Will you know it's happening? Well, you *should* be asked for consent to the process, but this does not always happen.

Pros and Cons: Having a comprehensive assessment can be useful where a child has complex needs – for example a disability that requires specialist input from several practitioners and multiple hospital appointments. Having someone to coordinate this can be extremely useful. However, the same problem described under Contactpoint also applies here: national, multi-user databases can never be fully secure. In addition, practitioners are asked to make a number of subjective judgments about your child and also about your own abilities as a parent. You may feel that this is highly intrusive.

What you can do: If a practitioner suggests carrying out an assessment of your child's needs, ask if it is a CAF and don't be afraid to refuse consent. Sometimes families are told that they will be unable to receive services unless they agree. This is called 'coerced' consent and if it happens, you might want to complain both to the Director of Children's Services in your local authority and to the Information Commissioner.

If you decide that it would be useful to have a CAF carried out, you can refuse to answer questions that you believe are irrelevant, intrusive or unnecessary and ask to see a copy of the final version before it is put on the eCAF database. You should also make regular Subject Access requests to see your child's entry on eCAF in order to check that the information is accurate.

National Pupil Database

What is it? This is a national database containing information about every child in a state school or nursery; private nurseries if any child's place is state-funded and any child or baby looked after by a childminder if their place is state-funded. The data is collected from schools via a termly schools census (or early-years census for under-5s) and includes information about academic progress, special needs, free school meals, behaviour, attendance and the child's means of transport to school. For more details about the school census, see:

<http://www.teachernet.gov.uk/management/ims/datacollections/schoolcensus/sc2010>

and the early-years census:

<http://www.teachernet.gov.uk/management/ims/datacollections/eycensus/>

Will you know it's happening? You should receive a 'Fair Processing Notice' telling you what information is being taken, but your consent is not sought and you cannot prevent upload of the information.

Pros and Cons: The information is useful in that it provides the government with a means of planning funding provision, but until 2000 this was achieved by collecting aggregate (anonymised) data from schools. There has never been an adequate explanation for the change over to personal data collection. The National Pupil Database is now used automatically to supply information to Contactpoint.

What you can do: Although you cannot prevent your school from supplying this data, you should make regular Subject Access requests to check its accuracy.

Managing Information Across Partnerships – MIAP

What is it? This is related to the National Pupil Database and is a permanent, lifetime education record for everyone aged 14 and over. Information collected in the school census about over-14s is automatically loaded into MIAP, and a Unique Learner Number is issued to each new database entrant. For more information, see: <http://www.miap.gov.uk/>

Will you know it's happening? Again, a Fair Processing Notice should be issued but the process is automatic and no consent is sought.

Pros and Cons: The idea behind MIAP is to provide a means of recording academic attainments throughout everyone's life, dispensing with the need to collect certificates and other 'proof' of education. It is envisaged that everyone will be able to produce their own curriculum vitae to show to employers, but concerns remain that those applying for jobs will be put under pressure to disclose the entire record, rather than just the 'sanitised' cv. It potentially makes life more difficult for young people who go through a bad patch.

What you can do: Encourage your child to check the accuracy of the data and correct any inaccuracies promptly. This is particularly important because it is a lifetime record that will be used for future employment and further education applications. (NB by the time your child is 14, any Subject Access request must normally come directly from him/her).

Connexions

What is it? A combined careers and welfare service for 13-19s designed to monitor young people for signs of problems that may affect their educational progress. Databases in each local authority take information about young people directly from each school and keep it on their Connexions Customer Information System.

Will you know it's happening? Section 117 of the Learning and Skills Act 2000 allows you to forbid the supply of any information to Connexions, other than name and address. If your child is under 16, the school should tell you and give you the opportunity to do this. Those over 16 must opt out for themselves.

Pros and Cons: The Connexions service was set up to reduce the number of young people not in education, employment or training. Originally it was centrally funded, but since 2008 responsibility has been left to local authorities and there have been repeated questions over Connexions' future. In many ways, Connexions' information-gathering function has been superseded by Contactpoint, eCAF and MIAP.

What you can do: Before your child turns 13, write to the head teacher of your child's school to request that they do not supply information to Connexions. If you and your child decide not to do this, at least ensure that your child makes regular checks on the information that is held.

Integrated Children's System

What is it? This is a local electronic social care case record system, recording all contact between your child and social services.

Will you know it's happening? If your child has contact with social workers for any reason, they will be entered on the local ICS system.

Pros and Cons: It makes sense for social workers to have an efficient case-management system and access is very limited. However, over the past few years there have been serious problems with the original specification set by central government and most local authorities are now beginning to re-design their systems to reflect what social workers actually need. You can find out more on the ARCH blog: <http://archrights.wordpress.com/2010/03/24/the-short-and-disastrous-history-of-an-it-project/>

What you can do: keep a check on the accuracy of records, but be aware that subject access can be denied if information relates to child protection investigations.

NHS Databases

Many people talk about 'the NHS Database', but in reality there is a whole network of systems. We strongly recommend visiting the Big Opt Out website for an explanation of these:
<http://www.thebigoptout.com>

Summary Care Record

What is it? GPs are currently being asked to upload a summary of every patient's health record to this national database. Once on the system, records will be available to *all* NHS staff.

Will you know it's happening? Your GP should write to you to give you the opportunity to opt out of having your/your child's record uploaded to the database, but be aware that in some areas GPs are being told to interview older children without their parents before agreeing to this opt-out. (See 'consent' below for more information).

Pros and Cons: The government's publicity leaflet says that being on the database will be useful if, for example, you are admitted unconscious to an A&E department (assuming they are able to discover your name). However, your medical record contains highly sensitive information and, as with any national database, security cannot possibly be guaranteed. Indeed, there have already been a very large number of security breaches on NHS systems.

What you can do: Go and read the information on the Big Opt Out site and then, rather than waiting for your GP to contact you, use their downloadable letter to opt out now. If you have any problems, their advice service is excellent. Here are the details:
email: admin@thebigoptout.com phone: 0845 8052 593

The National DNA Database (NDNAD)

What is it? Any child over the age of 10 can be arrested on suspicion of a criminal offence. If your child is arrested, a DNA sample will be taken. This is then sent to a laboratory to create a DNA profile which is entered on the National DNA Database. It is estimated that around one-quarter of the profiles on NDNAD relate to those who have not been convicted of any offence.

Will you know it's happening? Maybe. On arrest, the police will request cooperation in taking the sample using a mouth swab. If this is refused, the police can take it by force, usually by pulling some hairs from the child's head. Some people, including children, do not realise that the mouth swab means their DNA is being taken.

Pros and Cons: The government claims that keeping the DNA profile of everyone who is arrested can lead to better crime detection, but in fact the detection rate has not changed since the introduction of this policy in 2004. A European Court of Human Rights judgment in 2008 found that keeping profiles of innocent people indefinitely is a breach of human rights, and the new Crime and Security Act 2010 provides that under-18s profiles will be removed after 3 years (6 years for adults).

What you can do: The position is uncertain. If your child has been arrested but not proceeded against, write to the Chief Constable requesting removal of their profile from NDNAD. More advice and information is on the 'Reclaim Your DNA' website: <http://www.reclaimyourdna.org.uk/>

The Youth Justice System

If your child does get into trouble, information will be gathered via one of two personal-profiling tools and or the Common Assessment Framework already described.

ONSET

What is it? This is an assessment carried out by a local authority Youth Offending Team, said to 'predict' the likelihood of a child becoming an offender. A child may be referred by their school, the police or other agencies because of bad behaviour, persistent truancy etc. If the ONSET score purports to show a risk of future offending, the child will be referred to an intervention project.

Will you know it's happening? You should do because this is a voluntary process. In practice, some YOTs do not even say that the assessment is taking place, let alone ask for consent.

Pros and Cons: This is a highly controversial process and many leading academics and practitioners have dismissed the notion that future offending can be predicted in this way.

What you can do: If your child is referred to the local Youth Offending Team but has not been prosecuted, ask specifically if they are carrying out an ONSET evaluation. You can withhold consent to the process.

ASSET

What is it? This assessment tool is used when a child has committed an offence. The child's ASSET score is used to predict the likelihood of future re-offending and to make sentencing recommendations to the courts. It is an automatic process when a child is charged with a criminal offence and you have no influence over it whatsoever.

More information about ONSET and ASSET processes can be found on the Youth Justice Board website:

<http://www.yjb.gov.uk/en-gb/practitioners/Assessment/>

Fingerprint systems in schools

What are these? These are school library, canteen and registration systems that use pupils' fingerprints instead of a swipe card. To register a child on the system, their fingerprint is taken and converted into a string of numbers that is then stored on the database. In future, the child uses the system by placing their finger on an electronic reader.

Will you know it's happening? Well you should do but, in practice, many parents have only discovered by chance several months after the event that their child's fingerprint has been taken.

Pros and Cons: Schools say that these systems speed up queues, make it less obvious when someone is getting free school meals and do away with the problem of lost swipe cards. Convenient though this may be, it is getting children used to giving up their fingerprints for relatively trivial reasons when we should really be teaching them that this type of biometric

information should be guarded. It is important and irreplaceable. Although companies insist that fingerprints can't be reverse-engineered from the string of numbers, this is largely irrelevant - the police, for example, could still use the system to identify children. The government has not commissioned any research into the implications and security of the systems, and schools appear to be relying entirely upon the assurances of those selling the systems to them.

What you can do: If your child's school is introducing a biometric system, tell them that you do not want them to take your child's fingerprint and that they must instead use a swipe card. Some head teachers have attempted to prevent children from using the canteen if they do not provide a fingerprint, but the government has said that they cannot do this. If your child's fingerprint has already been taken, contact the school and ask that it is removed from the system. The Information Commissioner has said that it is not enough simply to press 'delete' – the data must be properly 'cleansed' from the system.

CCTV and Webcams

What is this? Many schools use CCTV to monitor their boundaries for security purposes, but some have gone much further and use CCTV to monitor children in the classroom and in school toilets. Some schools use IP Video which can be monitored from a control centre based elsewhere.

Will you know it's happening? A good question: anyone using CCTV should put up a notice to let people know, but many schools seem to have overlooked this.

Pros and Cons: Some schools seem to think it's a good idea to keep children under constant watch but, as with taking fingerprints, it is getting children used to a level of surveillance that few adults would tolerate in their own workplace. The Information Commissioner has issued guidance on the use of CCTV: http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx and says that CCTV should only be used in toilets 'in the most exceptional circumstances' but, so far, no action has been taken against schools that do this. The systems are expensive and the money could be put to far better use.

What you can do: Some schools have been forced to remove cameras that they installed without any consultation because of strong protest by parents and pupils. If your school is planning to introduce classroom and/or cloakroom monitoring, make your objections to the school governors and talk to other parents. A combined protest can be very persuasive. If the school has already installed CCTV and you believe that it does not comply with the guidance, make a complaint to the Information Commissioner.

Nursery Webcams

What are they? Some nurseries have installed webcams that allow parents to log in and watch their children over the internet.

Will you know it's happening? Hopefully, all nurseries using this system ensure that all parents are aware of it, but you might want to check if your child goes to a new nursery.

Pros and Cons: The idea is to give parents reassurance that their child is OK, but the webcam shows the whole room and everyone in it. That means you can see all of the children, and so can

anyone else with log-in details. Some nurseries even suggest that these details can be given to grandparents or other relatives. You may not think webcams are such a good idea for a number of reasons - and even the smallest baby has a right to privacy.

What you can do: If you object to the idea, choose a nursery without webcams and make it clear that you will object strongly if they are ever introduced. If your child is happily settled at a nursery that introduces webcams, it may be more difficult, but at least ask plenty of questions about the number of people who will be able to view the webcam images.

We hope that you now have a reasonably clear idea of the ways in which your child's data might be collected, but this isn't an exhaustive list – on other occasions you or your child will be asked for information by companies, schools, the police or your local authority. Don't be afraid to ask some basic questions every time you are asked for information, and teach your child to do the same.

These are the questions you should always ask:

Why are you collecting this information?
How will it help my child if I give it to you?
Who else will see this information?
What will they use it for?
How long will it be kept?
Where will it be kept?
How will it be secured?
Will it ever be downloaded from the central system?
If so, why, and how will you make sure it cannot fall into the wrong hands?

If you are not satisfied with the answers, or you cannot see any reason why the information is necessary, then refuse consent. If your child has been asked for personal information at school and you believe that you should have been consulted, complain to the head teacher and/or chair of the governors, request that they destroy the data, and complain to the Information Commissioner if they don't do this.

It can sometimes feel intimidating to stand up for your child's data protection and privacy rights, but it is only by doing so that you can ensure information is secure and that your child's dignity is preserved. Local authorities, schools and companies must appreciate how important it is to treat other people's information with respect, and the more they are challenged, the more effort they will make.

In some circumstances you cannot refuse to supply information, or you may feel that it is helpful to your child to do so. If this is the case, you should still ask questions, and keep a check on what information is held.

Making a Subject Access request

A Subject Access request is a request to see all information that an organisation holds about you. It involves writing to the organisation with your request, giving your name and address plus any information that the organisation needs to find your records, and usually paying a fee of up to £10. Once you have done this, the organisation must give you the information within 40 days. Full information is on the Information Commissioner's website at:

http://www.ico.gov.uk/upload/documents/new_pia_handbook_html/access.html

If your child is a teenager, they will normally have to make the request themselves.

Subject Access requests about information described above should be sent to the following organisations:

Write to the Local Authority for information held on:

Contactpoint
eCAF
Youth justice systems
Connexions
Any local authority service

[Write to the Department for Children, Schools and Families](#) for information held on:

National Pupil Database

MIAP

[Write to your Primary Care Trust](#) for:

Information about health records

[Write to the Chief Constable](#) of your local police force for information on:

The local police information system

The Police National Database

To see whether your DNA profile is held on the National DNA Database

[If the information is not correct](#)

Write back to the organisation holding the information to say that there is an error; explain what this is and why you believe it is wrong. Send your letter by recorded delivery. If you cannot get the data corrected, contact the Information Commissioner's office and ask for their help. Here are their details:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire SK9 5AF

Tel: 0303 123 1113 (helpline open 9-5 Mon-Fri) email: casework@ico.gsi.gov.uk

[Consent](#)

You need to know about the circumstances in which your child can give consent in their own right, and without your involvement. In order to understand what the law actually says, we strongly recommend that you read ARCH's report, *'Protecting the Virtual Child: the law and children's consent to sharing personal data'* which can be downloaded from:

[http://www.archrights.org.uk/docs/NYA\(4\)arch_16.2.0%5B2%5D.pdf](http://www.archrights.org.uk/docs/NYA(4)arch_16.2.0%5B2%5D.pdf)

The Information Commissioner has said that a child from around the age of 12 can normally undertake their own Subject Access requests because it is desirable that children start learning about their data protection rights as early as possible.

Unfortunately, the government has said that this means that children can also consent to the sharing of their personal information from around this age. There is no basis in law for this assertion. Some local authorities have gone even further by insisting that any child aged 12 can automatically give valid consent without parental involvement, but this is just plain wrong. There is a very high test for determining whether a child under 16 can give valid consent. It is not dependent upon their age, but on a number of other factors that need careful consideration.

If you believe that your child has been asked to give consent without a proper assessment of their ability to do so, or in circumstances where you believe that you should have been contacted, you may want to seek legal advice and make a complaint to the Information Commissioner.

The information in this booklet has been prepared by ARCH (Action on Rights for Children), an internet-based organisation that focuses on children's privacy and data-protection rights. More information can be found on their website: <http://www.archrights.org.uk> and their blog: <http://archrights.wordpress.com/>

The booklet was produced as an extension from the feature documentary **Erasing David**, (www.erasingdavid.com) which was supported by the **Joseph Rowntree Reform Trust** (www.irrt.org.uk) and the **Channel 4 BRITDOC Foundation** (www.britdoc.org). David Bond (Director) receives a letter informing him that his daughter Ivy is among 25 million residents whose details have been lost by the government's Child Benefit Office, he begins a journey that will see him hounded across Europe. David soon discovers some alarming truths about what the government and private companies already know about ordinary citizens.