# Guidance Paper 6: Confidentiality, Privacy and the Protection of Children's Data

This guidance paper discusses issues of confidentiality, privacy and data protection in relation to the collection of information from or about children for research. It is Guidance Paper 6 in the series *The Ethics of Research Involving Children: Common Questions, Potential Strategies and Useful Guidance*.

## 1. Privacy, Confidentiality and Anonymity

Research participants are entitled to **privacy, confidentiality and anonymity**, but what do those terms actually mean?

- **Privacy:** this is the right to keep things 'private'. It is protected by international human rights law, in particular by Article 8 of the European Convention on Human Rights and Article 16 of the UN Convention on the Rights of the Child 1989.This means that personal information about research participants (their names, where they live, details of their family) are for the researcher's information only and should only be revealed to third parties with the **explicit consent** of participants (see Guidance Paper 2 on obtaining consent).

- **Confidentiality**: Confidential information usually comprises information that is not publicly known and is being disclosed to an individual (i.e. the researcher) with the expectation that it should not be disclosed to anyone.

- **Anonymity**: information disclosed in private or in confidence may be anonymised, i.e. redacted or changed so that that it will not be possible to identify those involved. In some cases, young research participants may want to have some means of identifying their contributions to research findings. Encouraging participants to choose their own pseudonyms may be an alternative, as it will still allow participants to do this without breaching their anonymity and confidentiality.

In some situations, it may not be possible to fully ensure the confidentiality and anonymity of research participants. For example, when researching in a group setting (e.g. using focus groups), participants will be known to each other, and it may be difficult, if not impossible, for the researcher to assure all participants that the data generated during those group discussions will remain within the group. Participants will need to be reminded of this fact prior to the research commencing and at appropriate points during the research. As far as possible, the researcher should also try to get participants to agree not to discuss information shared within the group with outsiders.

There are also some situations in which you will have an ethical and even legal obligation to breach the confidentiality of young research participants. This is where there is a safeguarding issue, for example; that the participant has disclosed information that they or someone else, are at risk, or are likely to be at risk of harm. This will need to be clearly communicated to participants prior to the research commencing and at appropriate points during the research (see Guidance Paper 3 on Safeguarding).

Alderson and Morrow identify two ethical questions that the researcher needs to ask him/herself when considering breaking confidentiality[1]:

- Have the participants been warned, before they consent, about the limits of confidentiality and about what kinds of information might have to be shared with others to protect them?
- If it is necessary to breach confidentiality? And has this been clearly discussed with research participants so that they understand why this has to happen and what the process will involve?

Overall, the most important thing is to communicate information about privacy, confidentiality and anonymity to children in clear, plain and age-appropriate language (see Annex 1a and 1b in Guidance Paper 2 for examples). **Consent forms/participation information sheets should include a clear explanation of how their data will be stored and used**. You must consider the use of child-centred ways of presenting this information, such as via diagrams, graphics, videos, etc. For an example, see this online animation explaining a research project about child friendly justice.

## 2. Data Protection and Children's Rights

In addition to the rights and ethics associated with privacy and confidentiality, the right to **protection of personal data** (including children's data) is protected by law. '**Personal data**' is information that can be used to identify a person. The landscape of data protection laws in the UK and EU has changed since the introduction of the General Data Protection Regulation (GDPR) in 2018. The GDPR has been supplemented by the Data Protection Act 2018 and its rules must be observed in relation to research.

The most important elements of the GDPR/DPA 2018 are as follows:

- Its rules regulate the 'processing' (ie, doing something with that personal data such as collecting, analysing, storing and sharing) of 'personal data' (ie, any information relating to a person such as

---

[1] Alderson, P. and Morrow, G. (2020) *The Ethics of Research with Children and Young People: A Practical Handbook* (2nd Edition) London: Sage, p.38

their name, location, physical, physiological, genetic, mental, economic, cultural, social and online identity (Art 4 GDPR)).

- Researchers must have a lawful basis for processing personal data. The lawful basis used by the university in research is usually:
    - **University research as a public task**: Under the Data Protection Act 2018, university research data falls within the definition of a public task but it still requires that data is processed legitimately. This means that the nature and purpose of the data being processed and the potential risks this poses to children must be proportionate, necessary for the purposes of the research and reasonable. It is important to note that although ‘public interest’ – and not ‘consent’ is likely to be the lawful basis under which personal data is held and processed for research, the ethical and common law requirements of consent are not reduced.

- Research is deemed to be a lawful basis for processing personal data, including ‘sensitive’ data, that is information revealing a participant’s racial or ethnic origin, their political or religious views, any health-related information, biometric or genetic information, or information about their sexual orientation or experiences (Art 9 GDPR).

- Research participants who supply data must be made fully aware of why they are being asked to do so and what it will be used for. This requires that they receive clear, accessible information in advance of being asked to supply any data.

- Data must be held and used only for the agreed purposes. It must not be disclosed to any person or organisation other than those mentioned to participants in the information provided.

- The data must not be held for longer than is necessary and if a participant withdraws their consent, all their personal data must be removed from the project records. Withdrawal of data however will not be possible once it is anonymised and this should be made clear to participants,

The GDPR offers enhanced protection in relation to children’s data. In particular, Recital 38 of the GDPR states that:

> *“Children require specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.”*

Younger children or those with particular learning difficulties or disabilities may be less able to understand the risks, consequences, and rights in relation to the processing of their data and therefore require more protection than older children. Often this is a matter of providing the child with clear, accessible information about the nature of the research and the way in which the data will be used.

Amongst other things, they should be told:

- Why and how their data will be anonymised
- How their data will be used in the research
- How data will be stored during or after the research
- Who will have access to their data
- In what situations their confidentiality may need to be breached
- Whether they can request for their data to be deleted or destroyed – and if so, how

The UK Data Service also recommends that written information about the above be provided to the child and to a responsible adult. Such information should include a contact telephone number and other details of the researcher(s). It is imperative that researchers acknowledge that data management can be complex and difficult for everyone to understand, therefore particular attention must be made to ensuring that this information is communicated in an accessible way.

## 3. Archiving and sharing data beyond the end of the research project

Sometimes, you may wish to store data obtained from child participants for future use, or to share them with other researchers via a data sharing platform, such as the UK Data Service. The main benefit of storing and sharing data is that it can be used to inform future work (which also benefits participants).

There are a few questions to think about in deciding whether or not to make data available for future use:

- Is there a substantial public interest, and will this outweigh data privacy?
- Is the data sensitive or non-sensitive? What constitutes ‘sensitive’ data is defined in Article 9 GDPR as data:

  > *“…revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and…genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.”*

- The more sensitive the data collected is, the more safeguards should be put in place if it is to be used again in the future. Some consideration should be given to whether children (rather than adults) would view the data as sensitive.
- In cases of non-sensitive data, you should still include a research plan for data sharing in your ethics application.

- Regardless of whether the data is sensitive or non-sensitive, researchers should consider whether data should be anonymised so that participants cannot be identified in future studies without their consent. However, there may be circumstances where there is a need to be able to identify participants for welfare reasons if accessing the data again.

If you plan on archiving or storing the data obtained from children after the completion of the research project, you will need to ensure that your child participants consent to this.

**UK Data Service, The General Data Protection Regulation (GDPR): Research and Archiving FAQs:**

> *“The best way to achieve informed consent for archiving and data sharing is to offer the participant the option to consent (on a* ***granular level****) to what will be included in the archiving process and seek to* ***identify*** *and* ***explain the possible future uses of their data****.*
>
> *“How might this look in practice? In a qualitative study, this could be achieved by allowing the participant to decide which parts of their input to the study can be archived for future reuse, such as: the anonymised transcripts, the non-anonymised audio recordings and the non-anonymised photographs.”*

Participants may sometimes change their minds about the sharing of data. Article 17 of the GDPR gives both adults and children the right to have their personal data erased in some specified circumstances where, although the original collection and processing may have been compliant with the GDPR, continuing to hold their personal data against their wishes is not. This is sometimes referred to as the ‘right to be forgotten’. In such situations, children should be clearly informed of how or if they can withdraw their data after the study; and advice should be sought from the university research ethics team and the university legal team.

A final consideration here for researchers is ownership of data, particularly given that creative methods may involve the child producing something or submitting written or visual contributions. Researchers must be clear whether they own the data or whether it should be returned to the participant afterwards, for example if photographs are taken of the materials.

## 4. Checklist

The following is a summary of some of the factors to consider in relation to confidentiality, privacy and data protection in research involving children:

- ☐ **Legality**: Am I acting in a way that is legally and ethically correct when it comes to maintaining confidentiality, safeguarding, data protection and data sharing?

- ☐ **Anonymity and confidentiality:** Have I assured participants that they will not be identifiable from their research data? Has the data been appropriately anonymised?

- ☐ **Breaching confidentiality:** Have I clearly explained to participants that if they choose to reveal information that raises concern, I will have a duty to disclose this to someone?

- ☐ **Usage:** Have I clearly explained to participants how their data will be used?

- ☐ **Storage:** Have I clearly explained to participants how, where and for how long their data will be stored? If this was data about myself, would I be happy for it to be stored this way?

- ☐ **Sharing:** Am I going to be destroying the data after the project, or will it be made available to others for future research projects? In deciding between these options, have I considered what implications this may have for the participants? Have I sufficiently anonymised the data prior to sharing?

- ☐ **Ownership:** Who owns the research data collected? E.g. if you have collected drawings, diagrams, etc from children, will you be returning it back to them?

- ☐ **Withdrawal:** Is it possible for participants to withdraw their data from the research? Has this been communicated to them? If they can withdraw, have they been told how they can withdraw their data?

- ☐ **Complaints:** Does the child know who to contact and how if they are concerned about any aspect of the data management in the research? Have I also made this information available to a responsible adult?

- ☐ **If in doubt about whether your ethics framework complies with data-protection rules, contact your university data protection office.**

## Useful resources

- Information Commissioner’s Office: How does the right to erasure apply to children?
- ICO, Key Data Protection Themes: Children
- UK Data Service, Guidelines on Consent for Data Sharing
- UK Data Service, The General Data Protection Regulation (GDPR): Research and Archiving FAQs