Case Study on Privacy and Research Ethics in Public Records

This seminar task asks us to analyse a short case study about a government records clerk, a researcher, and access to identifiable property tax data. We will identify the key ethical and legal issues in each decision point, focusing on privacy, informed consent, and proper handling of personal data. Our answers link these decisions to relevant UK and European frameworks, in particular the UK GDPR, the Data Protection Act 2018, ICO guidance, and professional codes of conduct.

The Case

Ricardo works for the records department of his local government as a computer records clerk, where he has access to files of property tax records. For a scientific study, a researcher, Beth, has been granted access to the numerical portion "but not the corresponding names" of some records.

Beth finds some information that she would like to use, but she needs the names and addresses corresponding with certain properties. Beth asks Ricardo to retrieve these names and addresses, so she can contact these people for more information and for permission to do further study.

Now consider, what are the ethical issues involved in deciding which of these options to pursue?

1. If Ricardo is not responsible for determining allowable access, should he release the names and addresses?
2. Suppose Ricardo were responsible for determining allowable access to the files. What ethical issues would be involved in his deciding whether to grant access to Beth?
3. Should Beth be allowed to contact the individuals involved? That is, should the Records department release individuals' names to a researcher? What are the ethical issues for the Records department to consider?
4. Suppose Beth contacts the individuals to ask their permission, and one-third of them respond giving permission, one-third respond denying permission, and one-third do not respond. Beth claims that at least one-half of the individuals are needed to make a valid study. What options are available to Beth?

Discussion and Answers

1. Ricardo not responsible for access: should he release the names?

If Ricardo is not the person authorised to decide access, he should not release names and addresses at all. The records contain personal data, so any disclosure must follow the controller's rules and the UK GDPR principles of lawfulness, fairness, transparency and purpose limitation, which say data should only be used for clearly defined purposes and under proper authority.

Beth was explicitly given only the numerical data, which is consistent with ICO anonymisation guidance that recommends removing direct identifiers such as names and addresses when sharing data for research. If Ricardo bypasses this and shares identifiers on his own, he is likely breaching both data protection law and professional ethics, since the BCS Code of Conduct says members must not disclose confidential information without permission from the relevant authority.

2. If Ricardo *is* responsible for access: what ethical issues arise?

If Ricardo is the decision maker, he has to judge whether sharing identifiers is legally allowed and ethically acceptable, not just whether it helps the study. Under UK GDPR and the Data Protection Act 2018, research is recognised as a valid purpose, but any research processing must still comply with the core principles and have a clear lawful basis, such as a public task plus specific research provisions with safeguards.

He also has to apply data minimisation (only sharing what is necessary) and consider whether Beth really needs full names and addresses, or whether pseudonymised data or an intermediate contact process would be enough, as stressed in GDPR Article 5(1)(c) and guidance on anonymisation and pseudonymisation. Finally, ICO research guidance expects proper governance, for example documented purposes, risk assessment and appropriate safeguards, so Ricardo should involve a Data Protection Officer or similar role before approving such access.

3. Should Beth be allowed to contact individuals, and should names be released to her?

Whether Beth may contact individuals is ultimately a decision for the Records department as the data controller, not for her or Ricardo alone. UK and EU guidance accepts that public bodies can use personal data for research, but it must be done in a way that is lawful, fair, transparent and proportionate, with special care over direct contact with citizens whose data were originally collected for another purpose.

A common ethically safer approach, consistent with ICO and research governance guidance, is for the Records department to keep control of names and send information or invitation letters on Beth's behalf, rather than handing her the full identified list. This protects privacy, keeps the department accountable, and aligns with professional codes such as the BCS Code of Conduct, which emphasise respect for privacy and not disclosing confidential information without proper authority.

4. One third consent, one third refuse, one third do not respond: what can Beth do?

In this situation, the only people Beth can treat as participants are those who explicitly gave permission. Under GDPR, consent must be a clear, affirmative act, and Recital 32 and ICO consent guidance both state that silence, inactivity or pre ticked options do not count as valid consent, so non responders cannot be counted as if they had agreed.

Beth must also exclude those who explicitly refused, as their wishes are clear. Her realistic options are to proceed with the smaller consenting sample (and possibly reassess the study design), send one reminder to non responders and still treat non reply as "no", or redesign the project so that more of the analysis uses anonymised data that do not require ongoing consent, as recognised in ICO anonymisation and research guidance. What she cannot ethically or legally do is "top up" her numbers by including people who did not respond.

References

BCS, The Chartered Institute for IT 2022, *BCS Code of Conduct*, BCS, viewed 14 November 2025, https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/.

European Commission 2025, *Data protection explained*, European Commission, viewed 14 November 2025, https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en.

European Union 2016, *Regulation (EU) 2016/679 General Data Protection Regulation, Article 5 and Recital 32*, viewed 14 November 2025, https://gdpr-info.eu/.

ICO 2025, *Principle (a): Lawfulness, fairness and transparency*, Information Commissioner's Office, viewed 14 November 2025, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/.

ICO 2025, *What is valid consent?*, Information Commissioner's Office, viewed 14 November 2025, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/.

ICO 2024, *The research provisions (UK GDPR and DPA 2018)*, Information Commissioner's Office, viewed 14 November 2025, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/the-research-provisions/.

ICO 2023, *Introduction to anonymisation*, Information Commissioner's Office, viewed 14 November 2025, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/anonymisation/.

UK Government 2025, *The UK's data protection legislation (UK GDPR and Data Protection Act 2018)*, GOV.UK, viewed 14 November 2025, https://www.gov.uk/data-protection.