University of Edinburgh IoT Initiative Principles v1.1c

Publish date: 09/05/2018
Authors: Charles Raab, James Stewart, Andres Dominguez, Ewan Klein, Simon Chapple

The information in this document is subject to change without notice. You can check for the latest version at the iot.ed.ac.uk website.

This document version is for Phase 1 launch of the IoT Service at the University of Edinburgh.

Overview

The University of Edinburgh Internet of Things (IoT) Initiative, which includes the IoT Research and Innovation Service, should meet, and be perceived as meeting, high standards for governance for the use of the IoT infrastructure. This includes reconciling ethical and legal rules about data with the exploration and application of the Service for social benefit. It should also seek to include the involvement in governance and development of those whom the Service will affect.

Fundamentally, the Service must comply with all applicable legislative requirements, such as the General Data Protection Regulation (GDPR) or its equivalent in UK law, environmental protection, equality and dignity, and protection of vulnerable people, and safeguard the reputation of the University in relation to IoT-enabled projects and their implementation. It must also protect the rights and freedoms of those who are potentially affected by the use of the Service's processes. The Governance and Ethics Action Group (AG) will support the appointed officers in the University who are responsible for research ethics and data protection.

Research is done for diverse reasons by diverse actors in diverse contexts. These principles and procedures apply to all users of the Service, including those conducting R&D to develop novel public or commercial services. This document sets forward a set of procedures and principles that relate to the governance of the IoT infrastructure. The principles are articulated at a high and general level, derived from a range of contemporary developments in the use of personal data, and are not unique to IoT.

This document is a work in progress that aims to put in place procedures to help all researchers to abide by the spirit and letter of the principles. The University's IoT Initiative will use formal compliance evaluation, expert advice, and consultation and participation to govern and inform research using the Service, to review the principles, and to develop further the procedures and support mechanisms. The IoT Initiative will support individual projects and researchers to contribute to a common debate about what we *should* be doing as much as what we *can* do with technology and data.

General Principles

These principles apply to the IoT Initiative, which subsumes both the Research and Innovation Service and any projects that use the service. All projects involving the use of personal data will be expected to comply with applicable data-protection law; in particular, with the more specific and well-established set of data-protection ('fair information') principles embodied in such law. That set has its roots in ethical norms and values that may be insufficiently emphasised in law, or may be outside the scope of data-protection law. Beyond legal compliance, IoT projects should therefore aim to determine whether, and how, data-protection and other ethical principles are relevant to the specific circumstances of a project, how to take them into account, and how to implement them within the project. The following principles apply to the means by which an IoT project is conducted, including the processing[1] of data, and to the use of the research or practical outcomes of the process, and include[2]:

- consistent with norms embodied in human-rights principles, individuals should be treated as ends, not means, and are entitled to have their dignity and autonomy respected.
- individuals should not suffer physical or psychological harm from IoT projects.
- adverse effects beyond the individual (e.g., groups, categories of persons, society in general, or the environment) should be avoided or mitigated.
- there should be equal access to the benefits accruing to individuals.
- benefits from the application of IoT should accrue to the common good and not only to research or operations management.
- the necessity and proportionality of an IoT process should be considered and capable of being demonstrated.
- because the IoT Service's demonstrable trustworthiness is crucial for public trust, IoT research and service-related applications should be conducted with high levels of transparency and accountability by means of explicit and auditable procedures.
- IoT projects should aim to mitigate the adverse impacts that data processing may have on individual privacy and on other individual and social values.
- IoT projects should seek to minimise any negative impact on the environment. This includes the animal and insect life, flora and fauna, and also the built environment, in all of their implementation, construction and ongoing operation.

Procedures

1. All projects should go through the appropriate ethics and privacy assessment processes already in place in the University. This may differ for each school.

[1] Following the meaning of 'processing' in data protection law (e.g., the General Data Protection Regulation, Article 4(2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

[2] The word 'should' is used in these principles because there may be valid reasons in particular circumstances why a principle may legitimately be overridden, but the implications of overriding must be understood and carefully considered.

2. All project developers should complete a checklist of ethical and legal issues before starting to use this service. This will help identify whether the project will collect or use personal data, requiring a PIA, identifies issues of equality impact, involve children or other vulnerable people, or have environmental impacts. Projects can be phased, so that technical developments are made before moving on to using 'real life' contexts and data. In Phase 1 the Service will not accept new projects that might collect personal data.

3. If your project does not conform to the ethical principles outlined in this document, then you must provide documented reasonable argument for why this is the case and why it is deemed acceptable to proceed with the project. You must keep a **record** of your application of the above processes to demonstrate due ethical diligence for your project. This **record** should be in the form of a list of ethical review processes that have been successfully applied with dates of sign-off and links to the supporting documentation. This record must be presented to the IoT Service team for their review prior to your project being permitted to use the IoT Research and Innovation Service facilities.

4. The University's IoT Initiative is committed to being open, transparent and accountable about the 'who, what, where, when, why and how' of data collection and use. As part of ethical review, research projects and Service users should, where possible, involve and consult those directly using places and objects connected to the IoT infrastructure or who are reasonably likely to be affected by their use.

5. Service users are encouraged to share experiences of resolving issues of data protection and user engagement with the broader user community* of IoT developers to help in a) designing and reviewing the systems' use and governance, b) evaluating fairness, c) developing transparency and accountability procedures, and d) developing best practice resources and guidelines.

6. All complaints will be handled according to the published procedures of the University and partners, and reviewed using IoT Initiative governance processes

7. These procedures are included in the Terms of Use of the IoT Service which also include the requirement to abide by the University of Edinburgh Computing Regulations and the University of Edinburgh Security Policy, which in turn include other UoE ethical policies and/or codes.

Go / No Go Tests

The project does not:

- process information about living, identifiable individuals ('data subjects');
- adversely affect the values and goals laid out in the UoE Dignity and Respect Policy, or Equality Outcomes Action Plans;
- adversely affect values and goals of UoE in relation to the environment.

Reference Documents

http://ukrio.org/publications/code-of-practice-for-research/
https://www.ed.ac.uk/information-services/about/policies-and-regulations/security-policies/security-policy
https://www.ed.ac.uk/information-services/about/policies-and-regulations/computing-regulations
https://www.ed.ac.uk/equality-diversity/dignityrespect
https://www.ed.ac.uk/equality-diversity/about/legislation-policies