

<i>Written by</i>	Data Protection RTPI
<i>Date</i>	February 2019

---

# RTPI Data Protection Policy

## Contents

1. Overview.....	2
2. Data Protection Principles.....	2
3. How we define personal data.....	2
4. How we define special category data.....	3
5. How will we process personal data? .....	3
6. How should you process personal data for the RTPI?.....	3
7. How must special category data be processed? .....	5
8. Subject Access Requests .....	5

# 1. Overview

1.1 The RTPI needs to gather and use information or 'data' about individuals as part of its business. The RTPI intends to comply with its legal obligations under the Data Protection Act 2018 (the '2018 Act') and the General Data Protection Regulations (GDPR) in respect of the processing of 'personal data' and 'sensitive personal data'. These rules apply whether data is stored electronically, on paper or on other materials.

1.2 This policy explains how the RTPI will hold and process this information. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of the RTPI.

1.3 This policy applies to all employees, volunteers, consultants, suppliers and anyone else working for or on behalf of the RTPI. It applies to all data that the RTPI holds relating to identifiable individuals and members.

1.4 If you are an employee, this policy does not form part of your contract of employment and it can be amended at any time.

## 2. Data Protection Principles

2.1 Personal data must be processed in accordance with the seven key GDPR principles. It must:

- be processed lawfully, fairly and transparently. There must be a lawful basis for processing data, personal data must be used fairly and we must be honest with people (employees and members alike) about how we will use their personal data;
- the purpose for which data is used must be clear from the start and this must be specified in our privacy information. We may only use data for its original purpose, if we have consent or if there is a lawful basis for doing so;
- data processing must be adequate, relevant and limited to what is necessary;
- reasonable steps must be taken to ensure that all data held is correct and up-to-date. If it is not, we must take reasonable steps to correct or erase it as soon as possible;
- data must not be kept for longer than is necessary;
- appropriate measures must be taken to ensure the integrity and confidentiality of personal data;
- RTPI is accountable for the data it holds and how it complies with all principles.

## 3. How we define personal data

3.1 'Personal data' means data which relates to an identified or identifiable individual. What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors. If it is

possible to identify an individual directly from the information you are processing, then that information may be personal data. If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. Even if an individual is identified or identifiable, directly or indirectly, from the data you are processing, it is not personal data unless it 'relates to' the individual.

## 4. How we define special category data

4.1 Special category data' is a type of personal data that the GDPR says is more sensitive and so needs more protection. It is broadly similar to sensitive personal data under the 1998 Act and consists of data relating to:

- The racial or ethnic origin of the person;
- His or her political opinions;
- His or her religious or other beliefs;
- Whether he or she is a member of a trade union;
- His or her genetics;
- His or her biometrics (where used for ID purposes);
- His or her health ;
- His or her sex life or sexual orientation.

There are separate safeguards relating to personal data about criminal offences and convictions and specific provision to process such data apply.

## 5. How will we process personal data?

5.1 The RTPI will process personal data (including special category data) in accordance with our obligations under the 2018 Act and the GDPR Principles in paragraph 2.

5.2 We will notify a data subject about the purpose for which we intend to process the personal data, who we might share it with and how the data subject can object.

## 6. How should you process personal data for the RTPI?

6.1 Everyone who works for, or on behalf of the RTPI, has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy. The RTPI's Data Protection Officer is responsible for reviewing this policy and updating the Senior Executive Team on the RTPI's data protection responsibilities and any risks in relation to the processing of data.

6.2 You should only access data covered by this policy if you need it for the work you do for, or on behalf of the RTPI and are authorised to do so.

6.3 You should not share personal data informally.

6.4 You should keep personal data secure and not share it with unauthorised people.

6.5 You should regularly review and update personal data which you have to deal with for work.

6.6 You should not make unnecessary copies of personal data and should keep and dispose of those copies securely.

6.7 You should use strong passwords.

6.8 You should lock your computer screens when not at your desk.

6.9 IT can advise about sending sensitive data outside of the RTPI, and you must contact them before doing so.

6.10 Do not save personal data to your own personal computers or other devices.

6.11 Personal data should never be transferred outside the European Economic Area without the consent of the data subject or the authorisation of the Data Protection Officer.

6.12 You should lock drawers and filing cabinets. Don't leave paper with personal data lying about.

6.13 You should not take personal data away from RTPI's premises without authorisation from your line manager or Data Protection Officer.

6.14 Personal data should be shredded and disposed of securely when you have finished with it.

6.15 You should seek the express consent of the data subject before using or disclosing sensitive personal data if you are authorised to do so, or if not, highlight to your line manager if you think additional consent is required.

6.16 You should ask for help from your manager or our Data Protection Officer if you are unsure about data protection or if you notice any areas of data protection we can improve upon.

## **7. How must special category data be processed?**

7.1 There are additional conditions on processing of special category data which must be met under the GDPR. This includes the express consent of the data subject. This will not normally be dealt with in RTPI and you should refer to the Data Protection Officer for advice.

## **8. Subject Access Requests**

8.1 Data subjects can make a 'subject access request' to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the Data Protection Officer who will coordinate a response.