GDPR: STAFF COMPLIANCE CHECKLIST

Asking for consent

Where consent is the most appropriate lawful basis for processing:

1. The request for consent is prominent and separate from terms and conditions.

2. People must positively opt in (no pre-ticked boxes or any other type of default consent)

3. The language is clear, plain and easy to understand.

4. We specify why we want the data and what we're going to do with it.

5. We give individual ('granular') options to consent separately to different purposes and types of processing (eg newsletters, info on specific medical topics).

6. We name our organisation *(and any third party controllers – not relevant)* who will be relying on the consent.

7. Individuals are told they can withdraw their consent to marketing or other communications, but that their medical records must be retained by law.

8. We ensure that individuals can refuse to consent without detriment.

9. We do not make consent a precondition of a service.

Recording consent

1. We keep a record of when and how we got consent from the individual.

2. We keep a record of exactly what they were told at the time.

Managing consent

1. We regularly review consents to check that the relationship, the processing and the purposes have not changed.

2. We have processes in place to refresh consent at appropriate intervals, including any parental consents.

3. We consider using privacy dashboards or other preference-management tools as a matter of good practice.

DRAFT

4. We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.

5. We act on withdrawals of consent as soon as we can.

6. We don't penalise individuals who wish to withdraw consent.

DRAFT