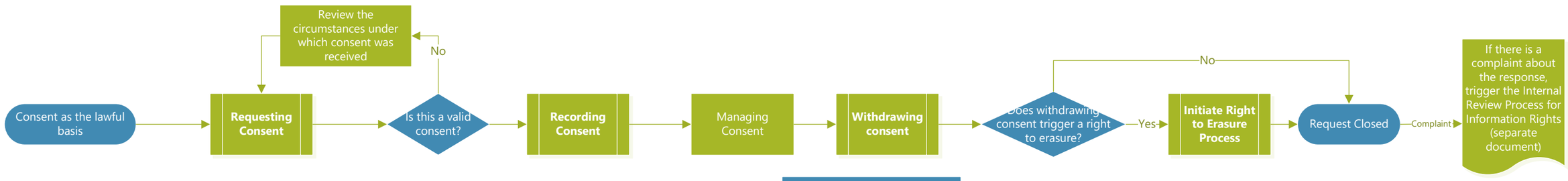
Title

Phase

Function



Consent as the Lawful basis

- Consent to the processing of personal data MUST be clearly distinguished from other matters (eg: not wrapped as a part of wider terms and conditions.
- Additional measures for consent relating to child in place?
- Is the processing reflected accurately in the Information Asset Register?
- Is a clear and unambiguous privacy notice specific to the purpose for which consent is being collected by be readily available (including where to find information on withdrawing consent)?
- If this collection will be shared with a third party, has the relevant due diligence checks been complete?
- Ensure that services that will use the personal data for ethically approved research, use public take rather than consent and where necessary provide the option of opting out of ethical research during time of collection.

Requesting Consent

- How is the consent being collected?
- Has Parental Responsibility consent been identified correctly for the child?
- Is the collection a clear affirmative action / statement?
- Silence is NOT consent.
- Avoid pre-ticked box

Is this a valid Consent?

- Is this freely given?
- Is the consent Specific?
- What steps will be taken to ensure that the data subject is properly informed of the purpose their personal data will be used?

Recording Consent

- Where will the consent be kept?
- The service relying on consent as the lawful basis can demonstrate how and when consent was obtained if audited

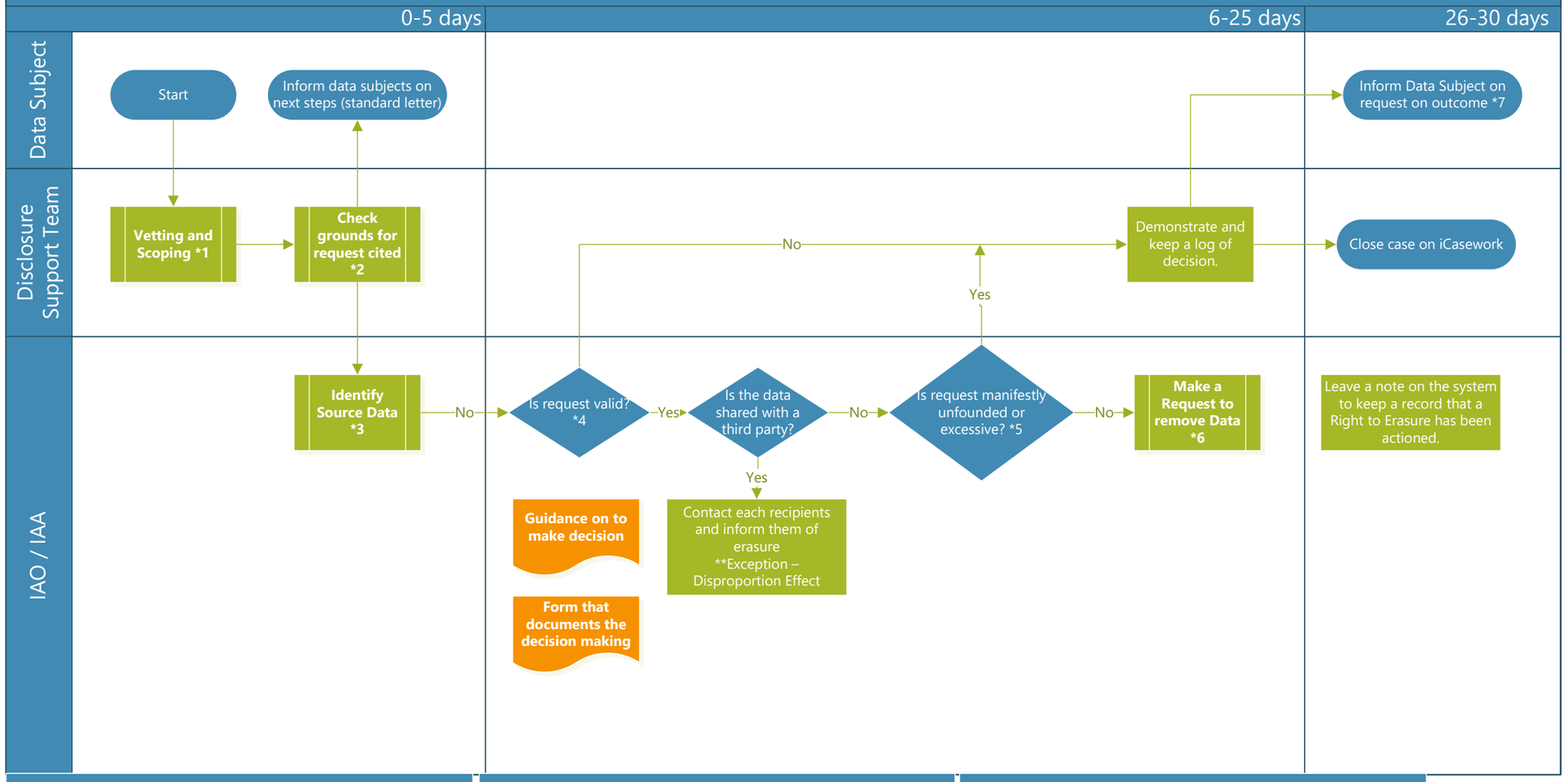
Managing Consent

- Consent is not time-specific, but if the process has been modified or altered has a fresh consent been taken?

Withdrawing Consent

- Keep a record that consent has been withdraw.
- Where the consent was collected for multiple purposes, the consent, the service will need to demonstrate that the processing for each of the processing has stopped.
- Notify any third party the personal data is shared that consent has been withdrawn.
- Where the right to withdraw consent triggers a right to erasure request, the erasure process should be initiated and a casework logged on icasework through the Disclosure Team. .

Right to Erasure – Meeting Article 17 requirements



*1 Vetting and Scoping

Disclosure Team to
- Check the Identity of the requestor.
- Check the Address of the requestor
- Check if data in scope is personal data.
- Check What information the requestor wants deleting.
- Check if the details have been provided to identify the information. If not, liaise with the requestor to identify the information. Onus is on the requestor to bring the information to the notice if the Trust.

*2 Check grounds for request cited

Disclosure Team to ensure that the requestor has cited the grounds for erasure.
Example:
- the personal data is no longer necessary in relation to the purpose for which it was originally collected;
- the processing is based on consent and consent is withdrawn (and there is no other legal ground for the processing);
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data was unlawfully collected;
- the personal data has to be erased in order to comply with a legal obligation;

Identify Servive area

*3 Identify the source data

Service area to:
- Check if the requestor has a legitimate right to make the request?
- Track all copies of the paper and electronic record
- Check if there any established relationships that will get affected if the record is deleted?
- Check if Information is held in backup systems (may stay on back ups untill over ridden), achieved systems as well as off site Storage?
- Check of there are any there party processors
- Understand if the request manifestly unfounded or excessive.

*5 Manifestly Unfounded

The Service must consider the request in the context in which it is made, and is responsible for demonstrating that it is manifestly unfounded.

The Servicemust not presume that a request is manifestly unfounded because the individual has previously submitted requests which have been manifestly unfounded or excessive or if it includes aggressive or abusive language. The service must consider the specific situation and whether the individual genuinely wants to exercise their rights.

*4 Is request valid?

Service Area to:
- The data is being used to exercise the right of freedom of expression and information.
- The data is being used to comply with a legal ruling or obligation.
- The data is being used to perform a task that is being carried out in the public interest
- The data being processed is necessary for public health purposes and serves in the public interest.
- The data being processed is necessary to perform preventative or occupational medicine. This only applies when the data is being processed by a health professional who is subject to a legal obligation of professional secrecy.
- The data represents important information that serves the public interest, scientific research, historical research, or statistical purposes and where erasure of the data would likely to impair or halt progress towards the achievement that was the goal of the processing.
- The data is being used for the establishment of a legal defence or in the exercise of other legal claims.

Please take advice from DPO or Legal Team if unsure.

Document in form

*6 Make a Request to Remove Data

Where the data has been made available in online environment:
- Inform the other data controller and take reasonable steps to take down the information.

Where the data is in electronic format on a system,:
- If a valid erasure request is received and no exemption applies then the service will have to take steps to ensure erasure from backup systems as well as live systems. Those steps will depend on how the Trust uses the data, retention schedule (particularly in the context of its backups), and the technical mechanisms that are available.
- The Service must be absolutely clear with individuals as to what will happen to their data when their erasure request is fulfilled, including in respect of backup systems.
- It may be that the erasure request can be instantly fulfilled in respect of live systems, but that the data will remain within the backup environment for a certain period of time until it is overwritten.
- The key issue is to put the backup data 'beyond use', even if it cannot be immediately overwritten. The service must ensure that they do not use the data within the backup for any other purpose, ie that the backup is simply held on the systems until it is replaced in line with an established schedule. Provided this is the case it may be unlikely that the retention of personal data within the backup would pose a significant risk, although this will be context specific.

*7 Inform Data Subject on outcome

When Request is refused the service must inform the requestor without undue delay and within one month of receipt of the request the following:
- the reasons the service is not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a different data controller.