ICO Trans policy and guidance

Document name	Trans policy and guidance
Version number	1.2
Status	Published
Department/Team	PADPCS, Info Access & People Services
Relevant policies	Dignity at work, Code of conduct, EDI policy, Accessibility and reasonable adjustments at work policy, Whistleblowing policy, Customer Service Adjustment policy.
Distribution	External
Distribution	The Annexes to this policy are for internal use only
Author/Owner	People Services
Approved by	Sarah Lal
Date of sign off	May 2023
Review by	May 2025
Security classification	Official

Key messages

The main objective of this policy is to:

- Provide support and guidance for individuals who wish to, have taken, or are intending to take steps to present themselves as a gender different to that registered at birth and those who identify as gender non-conforming (non-binary).
- Provide guidance for People Managers supporting colleagues who are transitioning or have transitioned.
- Provide guidance for staff handling cases containing protected information.

The ICO is committed to inclusivity and equity for trans and gender non-conforming people and to creating a culture in which employees, customers and stakeholders are treated with dignity and respect in which

they do not experience any kind of discrimination, harassment or bullying because of their gender or gender expression.

This policy and guidance sets out the framework and process to enable this to happen in a flexible and supportive way.

Does this policy relate to me?

This policy and guidance applies to all ICO staff, its stakeholders, and customers.

Table of contents

1. Definitions

1.1 The language around gender identity, presentation and transition is a constantly changing landscape. These are the key terms that we refer to throughout this policy.

- Trans – an umbrella term for those whose gender identity or expression differs in some way from the sex they were registered as at birth.
- Sex and gender – There is a difference between sex and gender. Sex refers to the physical characteristics of a person, such as male, female, and intersex. Gender is a separate concept that refers to an individual's personal gender identity which includes social, psychological, and behavioural aspects of being a man, woman, or other gender identity.
- Gender reassignment – The Equality Act 2010 defines in law the protected characteristic of 'gender reassignment' as someone who is 'proposing to undergo, are undergoing, or has undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attributes of sex.
- Transitioning is the term used to describe the process someone goes through to change from one gender to another with or without medical intervention. Every trans person's journey is unique and individual and not everyone who identifies as trans chooses to medically transition.
- Pronouns – Gender pronouns such as he/she/they/ze, is the pronoun that a person chooses to use for themselves to describe their gender.
- Non-Binary and genderqueer are the umbrella terms for gender identities that are not solely male or female.
- Cisgender (Cis) – A cisgender person has a gender identity that matches their sex assigned at birth.
- Gender non-conforming people are those who do not identify with a permanent binary gender identity, including those who identify in other ways e.g., non-binary, gender queer or gender fluid. This is not an exhaustive list and the term for gender identity is a personal one and will change from individual to individual.

- Gender Recognition Certificate is the document issued when a person has met the legal criteria under the Gender Recognition Act 2004 to allow them to legally change their gender on their birth certificate and related documents.

2. Introduction

2.1 At the ICO we consider equity, diversity, and inclusion to be essential to how we work. We aim to be inclusive in the way in which we deliver our services, protect, and inform the public, and employ, develop, and lead our people.

2.2 We are committed to fostering a diverse and inclusive workplace where all our colleagues have the opportunity to make a real difference. We are at our best when we support and look after each other, and when we trust and empower each other to be ourselves. Inclusive working environments are more productive, more creative, more representative, and more enjoyable. An inclusive workplace is in everyone's interests and is everyone's responsibility.

2.3 Fostering good relations – which includes promoting respect and understanding of rights between people with different protected characteristics, is a key element of the Public Sector Equality Duty within the Equality Act 2010 and section 75 of the Northern Ireland Act 1998.

2.4 All protected characteristics are important to us at the ICO, and we do not prioritise any one over the other. Trans colleague's customers and stakeholders fall under a protected group. This policy and guidance aims to ensure that the ICO is committed to creating an inclusive environment, where we embrace our inclusive ways of working, respecting each other and our stakeholders, customers and colleagues and treat all with dignity and respect.

2.5 The Equality Act 2010 makes it unlawful to treat someone less favourably because they are intending to, taking steps to, or have undertaken gender affirming surgery. The Act makes it unlawful to treat someone who is trans differently to other employees, customers, and service users or to refuse a service to them on the basis of their gender or gender expression.

2.6 The Gender Recognition Act 2004 (GRA) allows trans people, who are able to satisfy the GRA evidence requirements, to apply to the Gender Recognition Panel in order to seek full legal recognition of their acquired gender. If an applicant is successful, they will be issued with a full or interim Gender Recognition Certificate (GRC). A full GRC enables the person to obtain a new birth certificate which does not disclose the fact they have changed gender. The GRC also prohibits the disclosure of someone's gender history and the fact that they have applied for a GRC. Disclosure is a criminal offence. For ICO staff this means that we may commit an offence if we inappropriately share protected information even with other colleagues at the ICO. Only a small percentage of trans people hold GRC, and we therefore should not assume that every trans person has a GRC. Individuals are still able to transition and change their name, pronouns and how they identify without holding a GRC.

2.7 The ICO recognises that not all gender-diverse individuals may be legally reflected in the terms of the Equality Act or the Gender Recognition Act, but we are clear that they are fully encompassed within our inclusive workplace values and policies.

Back to Top

3. Guidance for ICO Employees

3.1 The ICO aims to ensure that its formal policies and practices are trans-inclusive and that legislative standards are upheld. This policy re-affirms the ICO commitment to a gender diverse workplace, helps all employees create and maintain a trans-inclusive culture and provides a step-by-step guide for people managers supporting a team member's transition.

3.2 This section applies to employees who plan to undergo any type of gender affirming surgery or who wish to identify as a different gender but are not intending to undergo affirming surgery.

3.3 The ICO is committed to supporting trans employees as their affirmed gender/identity from the time chosen by the individual concerned. Help and support is also available to those who wish to explore options regarding gender identity.

3.4 All trans and non-conforming employees have the right to choose whether to disclose their gender identity, to whom they disclose it and the circumstances under which they disclose it. The ICO encourages trans employees to disclose this information so that appropriate support, information, advice, and guidance can be provided if needed. If an employee makes the decision to transition or wants to explore options regarding gender identity, we suggest the first step should be to discuss this with their People Manager or the Inclusion and Wellbeing Team. If individuals do not feel comfortable discussing with their People Manager, they can contact the Inclusion and Wellbeing Team directly or a member of the People Services Team. The Pride Network are also available to offer help and support.

3.5 People Managers with the assistance of the Inclusion and Wellbeing Team will agree a support plan with the individual to provide a supportive and co-ordinated approach to the individuals needs. We understand that each individual's experience is unique, and the format of the plan should remain flexible, however as a guide the plan should include:

- A named contact from the Inclusion and Wellbeing Team.
- Key dates for medical appointments. This does not include details of the type of medical appointment but provides information relating to required time off for appointments and recuperation if required. When an individual is undergoing gender affirming surgery procedures, these will be recorded as absences, but will not count towards absence triggers.
- Whether and how this might impact on the individual's role, work patterns, performance etc.
- Following written permission from the individual, provide a summary of how and when the individuals information will be shared and managed.
- Changes to the individuals personal record, including email address and titles, detailing how and when these will change. These can be subject to change if the individual wants.

- Reasonable adjustments required to support any medical procedures needed for re-assignment, including counselling sessions.
- Guidance on the use of facilities. Individuals who have transitioned, are transitioning, or intending to transition from one sex to the other, have the legal right to use the facilities relevant to the sex they identify with. This protection is provided by the Equality Act 2010.
- What to do if facing transphobic abuse, bullying or harassment as a consequence of transitioning, through the ICO's Dignity at Work policy.
- Dates to review the progress of the plan.

An example of a Transition plan can be found in Annex A.

3.6 ICO Staff can support trans colleagues or individuals who are transitioning by;

- Interacting with your trans colleagues in ways that are respectful, friendly, considerate, and inclusive.
- Help create a positive and supportive work environment. In particular be mindful of the range of views and the need to contribute to an inclusive culture where all can thrive and offer their best. If you witness inappropriate behaviours, be prepared to address that, and politely explain your concerns or report to your people manager who may be able to support on your behalf.
- Be guided by your trans colleague and their preferences. It is important that you avoid making assumptions – even when your intention may be well meaning.
- Thinking of the person as being the gender that they want you to think of them as.
- Use the name and pronoun that the person asks you to. If you are not sure of the right pronoun, ask. e.g., "What name should I use?" or "How do you prefer to be addressed?"
- At the ICO, employees are free to include their pronouns in their email signatures and to ask colleagues to refer to them in that way. It is basic good manners to refer to somebody in the way that they prefer.
- Respect people's privacy. Do not ask what their 'real' or 'birth' name is. Calling a person by their previous name is

known as dead-naming, you must call a person by their chosen or preferred name.
- Do not ask about a colleague's surgery.
- Do not tell others about a person's trans status.
- Respect people's boundaries.
- Listen to the person and ask how they want to be treated and referred to and try to empathise with them.
- Understand the enormity of the step to change or present in a different gender to that recorded at birth and be supportive.
- You should also be sensitive around commenting to someone on their appearance or clothing. Your comment or compliment may be well meant and intended to be positive and supportive but that may not be how they receive it. There are no situations where making casual commentary to a third party about any individual's personal appearance is likely to be appropriate or conducive to a positive, respectful, and inclusive workplace.

3.7 Even if you are an experienced people manager, you may not have been in the position of supporting a trans colleague before. You may be concerned about making a mistake or saying the wrong thing. Guidance for managers on supporting a trans employee through disclosure and transition at work can be found in Section 4. Further specialised support is available through ICO Inclusion & Wellbeing Business partner, the Inclusion & Wellbeing Manager, and the PRIDE employee network group.

Back to Top

4. Guidance for People Managers

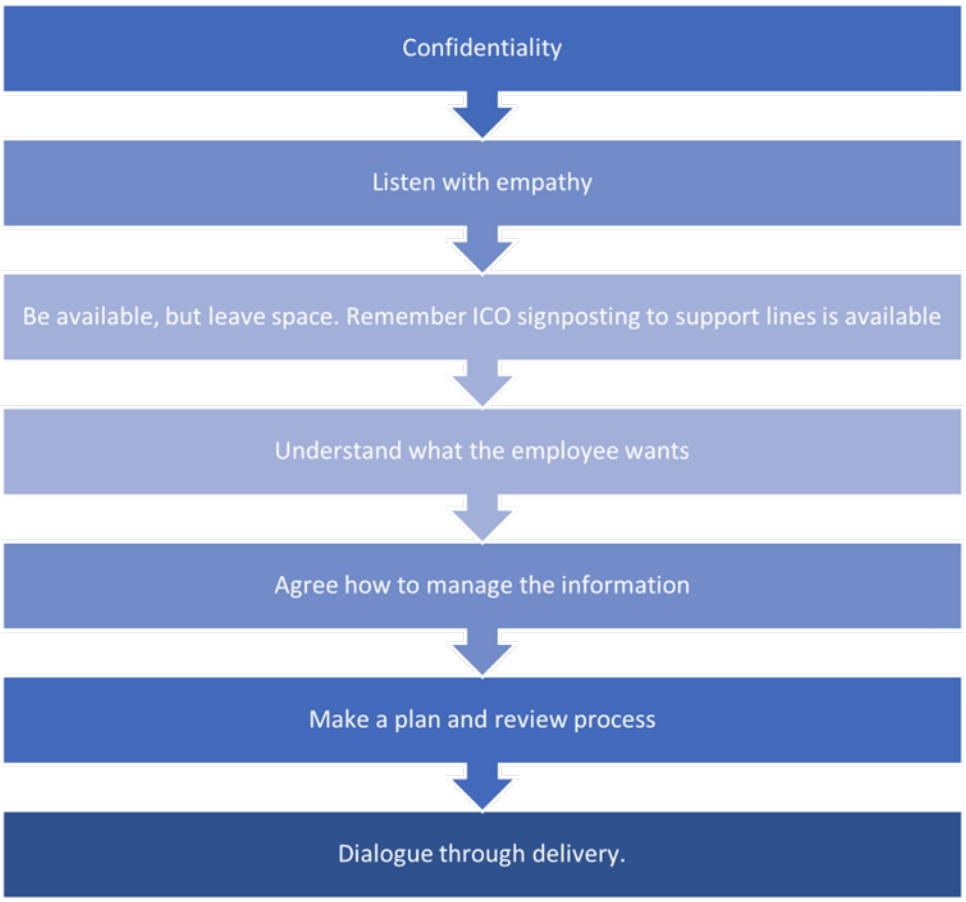
4.1 While there is often an assumption that the workplace transition of a trans employee is an HR issue, in practice, their people manager may have a more direct involvement, particularly at the early stages.

4.2 It is important that people managers understand what may be associated with this and are clear on both legal and practical responsibilities as well as how they might be most supportive to the employee.

4.3 If a member of your staff informs you of their intention to start a journey of transition or they disclose their gender history and/or current gender identity you should manage this sensitively and carefully.

4.4 Recognise that this step is unlikely to have been taken lightly. You should always be guided by the employee's views and preferences on how to proceed.

4.5 The following step-by-step considerations are intended to help you and inform your approach as a manager, but they are not definitive as each individual situation will be different. Although 'Confidentiality' always comes first, other steps may occur concurrently or in a different order.



4.6 **Confidentiality**

You MUST keep this information confidential and cannot disclose it to anyone else without the individual's consent. Remember that you should not even involve HR until the member of staff agrees that this may happen and when. If the employee discloses a gender history that includes them having applied for or obtained a Gender Recognition Certificate (GRC) then this information is given special protection and is known as 'protected information.' Section 22 of the GRA makes it a criminal offence for anyone who receives such information in an official capacity to disclose that information to an unauthorised individual – that includes another colleague at the ICO.

4.7 Listen with empathy

The individual may have been very unsure what reaction they would get, so an important first step is to listen carefully to what they have to say and offer reassurance. It is not your role to offer any form of opinion or judgement or to seek more information than the individual is willing to share at that point. You may wish to simply affirm that:

- you appreciate the individual sharing this information,
- you recognise that it may have been difficult for them to do so,
- you are happy to support them,
- you will collaborate with them and be guided by them in any next steps.

Try to avoid rushing into possible actions, observations or opinions which may be neither appropriate nor what the individual wants or needs.

4.8 Be available but leave space

Recognise that some individuals may wish to pause at this stage having taken a big first step in disclosing but not wanting to undertake further action immediately. Leave the timeframe for any future contact or action on the matter to them – while nonetheless demonstrating that you remain available and supportive as needed.

4.9 Understand what the individual wants

As an individual's trust and confidence in receiving a fair and appropriate reaction increases then you might start to explore together what the individual wants to happen. Trans people have a wide range of experiences and objectives. One employee may be planning a gender reassignment that involves significant medical intervention and surgery, while another may simply want you to be aware of their gender identity and to use different pronouns. Someone else may be informing you because they are concerned that they are already subject to inappropriate behaviour and unwanted treatment because of their existing gender presentation or presumptions about their gender identity and want to address this. Do not make assumptions but work in partnership with the employee to build understanding and explore ways forward.

Managers need to adopt an approach that meets the needs of the employee. They also need to be able to have a constructive conversation if what the employee wants is perhaps not reasonable or deliverable. This may be because of the existing legal framework, other legitimate constraints, a misplaced understanding, or the need to balance different rights. This is where the agreed involvement of those with specialist insight such as HR, the Inclusion and Wellbeing Team or Pride Network can be invaluable in achieving positive and sustainable outcomes for both the individual and the ICO.

4.10 Agree how to manage the information

Having clear and shared expectations about how the individual's information and any action that may arise from it will be handled will help build trust and confidence and avoid misplaced expectations and/or data breaches. You may want to explore and agree details around:

- Whether anything can be shared.
- What level of detail might be shared.
- What specific purposes information might be shared for.
- Who information may be shared with.
- When information might be shared.
- What actions or outcomes might be expected from sharing information.
- What the timescales for sharing are.

As a manager, while you may want to be able to get specialist advice on the specific issues from someone in People Services, you

would only be able to do this if the individual themselves gave you formal permission in writing. It is nonetheless reasonable for a manager to seek general information or guidance if it does not lead to indirect disclosure or identification of any individual.

Similarly, some internal actions might only be able to be taken with a certain level of disclosure. Working through the implications together of what is possible and what the employee wants will help deliver the optimum way forward.

4.11 Make a plan and a review process

Depending on what you have determined through the previous stages, it could be a good idea to agree a clear plan together as detailed in section 3.6.

If the plan is, for example to change an individual's name and pronoun you should meet and agree a plan on who needs to know, when and how they should be informed and under what circumstances. For example, some individuals may choose to inform their colleagues themselves in person or in writing, or they may prefer a designated colleague to do this for them. The plan should include how the individual would like to be addressed at which time and when records should change. Any personal data related to previous names or personal identifiers must be comprehensively updated.

Agree review meetings at an appropriate frequency that reflects the needs of the plan and agree how you will document your plan and review meetings and who will have access to that.

The plan must be entirely individually-led with trans staff having control over the whole process.

4.12 Maintain dialogue

Any plan will always be flexible to changing circumstances. If an employee is planning medical procedures, dates can change, and circumstances can alter. A trusting, honest and open relationship between a trans employee, their manager, and any specialist colleagues (such as HR) that may be invited into the process is important. This may involve joint problem-solving - like anticipating and planning for different scenarios or adapting agreed arrangements when circumstances change. An employee is not

under an obligation to disclose more than they wish but good dialogue will help to reduce misunderstandings.

Back to Top

5 Guidance for customers and stakeholders

5.1. ICO case officers can discuss any aspects of any trans related case with their manager or other appropriate colleague where it is necessary. However, any such discussions should meet the reasonable expectations of the trans person.

5.2 Cases can be handled following normal procedures, except where we have been explicitly told that they have obtained or have applied for a GRC, they have provided us with a copy of their GRC, or in some other way we have been actively informed that we are now holding protected information. If such cases are identified, it is the responsibility of all members of staff working on those cases to ensure that the protected information is handled appropriately.

5.3 In PADPCS, Team Managers (TMs) have been designated as points of contact for cases involving CRCs and trans members of the public. As such, they are expected to be fully familiar with the contents of this policy and to give advice on the procedure to staff dealing with trans and GRC cases.

5.4 TMs should identify Lead Case Officers and Case Officers who may assess, set up, monitor, and review potential trans and GRC cases. TMs should ensure that training is delivered and that case officers and other staff in the department are aware of how to recognise trans and GRC-related casework.

5.5 The procedure to be followed by PADPCS employees when dealing with a trans and GRC case can be found in Annex B – J. This guidance is for internal use only and not for wider publication.

5.6 The procedure to be followed by Information Access employees can be found in Annex K. This guidance is for internal use only and not for wider publication.

Back to Top

6 Further support

6.1 At the ICO the EDI board, EDI steering group and staff networks are committed to raising awareness and advocating EDI issues including those relating to trans people.

6.2 The Inclusion and Wellbeing Business Partner is our operational lead for EDI and will ensure best practice is adhered to.

6.3 The Pride Network aims to support positive representation, and the treatment of LGBTQ+ individuals and groups with dignity and respect.

6.4 Please see the dedicated IRIS pages for more information about the work of the EDI board and staff networks.

6.5 Further external sources of information can be found at:

- https://www.equalityhumanrights.com/en/advice-and-guidance/gender-reassignment-discrimination
- https://www.cipd.co.uk/knowledge/fundamentals/emp-law/sexual-orientation-discrimination/factsheet#15423

Whilst the ICO is not aligned to these organisations, you may find the following sources of information useful:

- https://www.stonewall.org.uk
- https://lgbt.foundation/
- http://www.gendertrust.org.uk/
- LGBT Foundation - Home
- Gender.Wales – Empower | Inform | Support
- TransgenderNI – Supporting and advocating for trans people in Northern Ireland
- Scottish Gender Identity Services - Scottish Trans
- Mindline Trans + | Mind in Somerset

Additional support can also be received through:

- BHSF counselling 24/7 support line – 0800 072 0353
- BHSF GP 24/7 call line – 0800 206 2576

Back to Top

7 Version history

Version	Changes made	Date	Made by
1.0	First draft	March 2023	People Services
1.1	Updated following feedback from TU's and staff networks. Reviewed by EDI Board	May 2023	People Services
1.2	Updated section 6.5 to clarify organisations that the ICO are not aligned with but may provide useful information	October 2023	People Services Approved by EDI Board

Back to Top

Annexes

Annex A. Example Transition Plan

Name of employee ……..

Name of point of contact …….

Completion of this transition plan is voluntary. It is up to you what information you feel comfortable to share. The contents of this plan will be kept strictly confidential and will not be shared more widely without your consent.

Likely areas that need to be discussed	Notes on discussions and any decisions (dated for clarity)	Who is responsible for actions identified? By when?
Have I settled on a preferred name and		

gender and when I want this to start from?		
What pronouns would I like to be known by?		
Do I want to/or am I ready to legally change my name and/or gender? What documents do I need?		
Do I want to medically transition (or already started)?		
Who do I now want to tell and how?		
How and when will personal information be updated?		
Do I need more support and information on gender identity?		
Do I need any adjustments to my workplace or working practices?		
Am I aware of the policies which support me?		
If I am considering surgery, are the timescales known?		
Key dates for appointments		
Who do I want to share this document with?		
Anything else to discuss?		

Back to Top

Annex B - PADPCS: Identifying GRC cases in sift. (Not for external publication)

If an email in the 'icocasework' queue on ICE contains protected information, the person processing that queue will download a copy of the correspondence and send it to the Protected Cases inbox.

If you are not sure whether the email contains protected information, it is fine to seek a second opinion from a relevant member of staff like an LCO or Team Manager.

Remember that just because someone self-identifies as trans, or mentions that they have transitioned, it does not mean that their correspondence automatically contains protected information. They should, however, continue to be treated with dignity and respect.

Once the email has been sent to the Protected Cases inbox, the person processing the 'icocasework' queue will then delete the email from their sent items and contact IThelp@ico.org.uk to have the original email deleted from ICE and the icocasework inbox.

Once the case has been created and the email has been added to the case, the officer delegated to work on the case will delete the original email from the Protected Cases inbox and will also delete the downloaded copies from their personal drives.

If an email has been added to the 'Protected cases' inbox that does not need to processed under the GRC procedures, it should be forwarded to icocasework@ico.org.uk. When forwarding the email please advise how the case should be dealt with in the body of the email.

If a GRC sift item is identified in the IR, DP, Public Advice or Business Advice sift queues in ICE it should be allocated to the delegated officers in the relevant sector.

The delegated officers will then create a case in the restricted area of SharePoint – download the docs from ICE, add them to the SharePoint case and then contact ICE help to have the sift item deleted from ICE and the icocasework inbox.

If an existing case was not initially identified as relating to GRC, but we discover it contains protected info, it should be flagged with a Group Manager.

Back to Top

Annex C. PADPCS: creating a GRC case. (Not for external publication)

GRC Cases will be dealt with on a restricted area of SharePoint. Access to this will be limited to delegated officers and managers in the PADPCs department.

Delegated officers will confirm that each case contains protected information related to a Gender Recognition Certificate. If it does not, it does not need to be restricted.

The process for setting up a restricted case is as follows:

- Find the relevant email(s) in the Protected Cases inbox. Save the email(s) to your desktop. Re-name the email – "DS to ICO (initial) DD/MM/YY"

- Create a new case (using +) on restricted area of SharePoint within the relevant month folder. Complete the following fields:

    - **Name** - Insert reference number* - Reference numbers will be sequential and will be formatted SGP000. You should use the admin log to determine the next reference.
    - **Description** - LEAVE BLANK
    - **Channel** - email or post.
    - **Date received** - date correspondence received.
    - **Preserved** - complete only if the case requires preservation (e.g., IICSA)
    - **GR Case status** - open/closed.
    - **Case closed** - LEAVE BLANK
    - **Case officer** - Name
    - **Security Class** - LEAVE BLANK
    - **GR case type** - Enquiry, Complaint, FOI, or info req
    - **Sector** - sector that the DC falls under.
    - **Sub-sector** - sector that the DC falls under.

- Make sure that you are in the relevant case folder in the restricted area of SharePoint. Upload the relevant email(s) from your desktop.

- Complete the following fields:
    - **Title** - LEAVE BLANK
    - **Channel** - email or post.
    - **Date received** - data correspondence received.
    - **Security class** - DO NOT CHANGE.

- After correspondence has been uploaded, make sure it is removed from your desktop.

Back to Top

Annex D. PADPCS GR Case Log. (Not for external publication)

The GR Case Log can be found in the GR Admin Log folder in the restricted SharePoint folder. Make sure you select edit document.

Details of all GRA cases should be recorded on the log:

- **Date received** - The date the initial correspondence is received.
- **Case reference Number** - Sequential starting SPG001
- **Case type** - Enquiry, DP/FOI complaint, Info request
- **Case Officer -** Name of delegated officer dealing with case.
- **Regarding** - Name of data controller
- **Status -** Open/Closed
- **Security check -** Document address/email check
- **Temporary access given -** Dates of temporary access given to IA or enforcement officers (only use for information requests and Enforcement case).

Back to Top

Annex E. PADPCS: Acknowledging the case. (Not for external publication)

The delegated officer should then send an acknowledgement, based on the templates provided in Annex M and following the email and postal instructions provided in this policy.

The acknowledgement will:

- Seek permission from the complainant to contact the data controller or any relevant other party about the case,
- Ask for the name of an appropriate individual within the organisation we can communicate with, and
- Give instructions as to how to send any further correspondence to us, to help us comply with our obligations under the GRA.

Whether we send it by email or post depends on how the customer contacted us. In general we should use the same channel that they used. Take no further action on the case until we receive the customer's response.

In the unlikely event that it is necessary to store hardcopy information, all case papers should be stored in an individual section of a secure filing cabinet. Case folders should be clearly marked "OFFICIAL – SENSITIVE-

PROTECTED INFORMATION". They should be marked with the names and job titles of those staff who may access the information, normally the case officer (once they have been allocated the case), and the Group Manager.

All correspondence sent to third parties should include the statement in Annex O drawing the recipient's attention to their duties under s22 of the GRA.

Back to Top

Annex F. PADPCS: email responses. (Not for external publication)

When sending email responses for a restricted case, you should follow this process:

Open the relevant email from the individual - "DS to ICO (initial) DD/MM/YY." Click reply (Do not select "REPLY ALL"). Double-check the email address is correct.

The email to the individual should be sent from the Protected cases account, not your individual email account.

- Change the sender to "protected cases."
- Select "options"
- Select "from"
- Change to casework.
- Remove normal outlook signature.

Draft the response using the templates as per Annex N.

The title of the email should be "[CASE REFERENCE] Response from Information Commissioner's Office." Once the security checks have been completed, and the acknowledgement/response has been checked – click send.

Go to your sent items (outlook) and save the email to your desktop. Save the sent item to your desktop. Rename the email "ICO to DS (acknowledgement) DD/MM/YY." Upload the relevant email(s) to the case from your desktop.

Complete the following fields:

- **Title** - LEAVE BLANK
- **Channel** - email or post.

- **Date received** - data correspondence received.
- **Security class** - DO NOT CHANGE.

When the email has been uploaded, remove it from your desktop.

Back to Top

Annex G. PADPCS postal responses. (Not for external publication)

When sending postal responses for a restricted case, you should follow this process:

Draft the response using the template found in Annex N. Once the security checks have been completed, and the acknowledgement / response has been checked, print the document using ICO logo paper.

Save the word document to your desktop. Rename the document "ICO to DS (acknowledgement) or (response) DD/MM/YY."

Upload the document(s) to the case from your desktop and Outlook sent items. Complete the following fields:

- Title - LEAVE BLANK
- Channel - email or post.
- Date received - data correspondence received.
- Security class - DO NOT CHANGE.

When the document has been uploaded, remove it from your desktop.

Back to Top

Annex H. PADPCS: Enquiry and Complaint cases. (Not for external publication)

Any subsequent correspondence from the individual should all be dealt with on the restricted area on SharePoint.

Standard complaint templates and enquiry LTTs can be used in any response. In the main the business-as-usual processes can be followed.

You must ensure:

- No correspondence relating to Gender Recognition cases should be kept on the case management system (ICE)

- No correspondence relating to the Gender Recognition cases should be left in protected cases inbox.
- Email responses should follow the process outlined in this policy.
- Postal responses should follow the process outlined in this policy.

When contacting Data Controllers, any correspondence we send to third parties should include a statement drawing their attention to their duties under s22 of the GRA, as per Annex O.

Back to Top

Annex I. PADPCS: Referrals to Enforcement. (Not for external publication)

Any formal regulatory action we take will focus on the procedures and practices adopted by the data controller for the handling of sensitive information, rather than the content of the material itself. In some cases, Enforcement may not need to know the identity of the person to whom the protected information relates, or the protected information may not be relevant to the investigation.

If a case needs to be referred to Enforcement, you should email a Group Manager who can consider whether any reference to the holder of the GRC or the protected information can be redacted without being likely to harm the Enforcement case and consult with the relevant Group Manager in Enforcement about that decision. If both conclude that redactions can and should be made, a Group Manager should make them.

Group Managers will then determine who will be dealing with the case. They will then:

- Complete the Request for Access – Restricted SharePoint template and send to ITHelp@ico.org.uk
- Ensure that the member of staff understands the procedure.

Temporary access to the restricted area of SharePoint will be arranged for the relevant case handler. Once access is no longer required an email should be sent to ITHelp@ico.org.uk requesting this is removed.

They should then pass the paper file to the relevant Group Manager in Enforcement, subject to the general principles in Annex L, updating the asset register and reassigning the ICE shell case.

The Group Manager in Enforcement will record receipt of the correspondence in the department's asset register, again making no reference to the content of the case and decide who will deal with it.

Case papers should be storied in an individual section of a secure filing cabinet. Case folders should be clearly marked "OFFICIAL – SENSITIVE-PROTECTED INFORMATION". In addition, they should be marked with the names and job titles of those staff who may access the information, normally the case officer (once they've been allocated the case), the Group Manager and the Director of Investigations.

If redactions were made to the file before passing it over, and either the case officer leading on the investigation or their Group Manager believes they require access to the full file, then they should discuss this with the Group Manager and/or the relevant heads of department if necessary. If there is dispute about the necessity or requirement to access the full file, the Director of Investigations and Head of PADPCS will make the final decision. Access to and movement of any additional material should be clearly recorded.

When writing to anyone in connection with the investigation, we should not make any reference to the GRA and/or the name of the GRC holder if it is not required to progress the investigation.

Back to Top

Annex J. PADPCS: Referrals to Information Access. (Not for external publication)

If you receive a SAR or FOI request on a GRC case, please contact: IAmanagers@ico.org.uk

IA managers will review the case docs, and then respond to ask you to send copies of the documents to one of IA's Support Officers, who will then set up a restricted case in IA's own restricted area.

IA managers and support officers will delete any documentation from their own outlook inboxes as soon as it is no longer necessary to hold it for the purposes of setting up a case.

Back to Top

Annex K. IA: general principles. (Not for external publication)

In Information Access, Team Managers and Group Managers can advise on GRC casework. Handling of restricted requests will be done by Senior Officers or experienced Leads.

GRC cases are set-up and held in the IA restricted area, in line with the IA restricted cases policy. Any issues with set-up or storage of cases should be raised with a Team Manager

If it becomes apparent that a case contains protected information only after it has been set up and worked on in ICE for some time, the case handler should flag this with a Team Manager.

Protected information in the IA inbox.

Support officers working the team inbox will flag GRC cases with Team Managers, one of whom will review to confirm that the correspondence contains protected information, and then a restricted case will be set up as soon as possible, and the original email removed from the inbox.

Handling trans and GRC-related SARs.

Once a restricted case has been set up, IA managers will then determine who will be dealing with the case. If necessary, they will contact IThelp@ico.org.uk to set up access to the IA restricted area.

The case handler will acknowledge receipt of the request. IA staff should make every reasonable effort to define and agree the scope of any information requests with the requester in order to reduce the risks associated with information being duplicated and disclosed. So, for example, if they have asked for "all data," it is appropriate for IA staff to explain that we usually do not provide requesters with copies of correspondence they have sent to us (which is likely to include their GRC).

The case should only be discussed in team queries meetings if it is possible to do so without disclosing the identity and/or GRC status of the requester.

Any correspondence regarding the case should follow the principles set out in Annex L. Case handlers should also review the other annexes and consider whether any of the template text should be included in their correspondence.

Existing procedures can be followed to identify who holds information relating to the data subject. However, no reference should be made to the GRC in consultation emails unless it is strictly necessary. Any consultation

that does require us to discuss protected info should be done in a focussed way – email individual staff directly rather than team inboxes, for example. When consulting with external organisations, consider whether it is necessary to send the notice contained in Annex O.

Where the requested information includes information relating to a GRC, IA will need copies. Copies should be sent in accordance with the general principles in Annex L.

If any of these records are held in hard copy only, and there is a pressing need for them to continue to be held only in hard copy, they will need to be transferred into IA's secure storage. They should be logged on IA's asset register, making no reference to the GRC content. Speak to IA's LIMO regarding this.

IA will agree with the requestor the means by which the information will be sent to them. Normally this will be by email, or through the post by Recorded Delivery. If a response needs to be sent by post and the person handling the request is not in the office on the day it needs to be sent, they should identify a colleague who is in the office and contact them directly to organise printing and posting. Do not put documents containing protected information in the "Post Responses – For Printing" folder of the team inbox.

Consideration should be given to providing a further level of security to email disclosures by password protecting them. If the requestor expresses particular views on disclosure (i.e., they request that we provide them with a USB stick or something similar) we should accommodate them if possible.

Back to Top

Annex L. General information handling principles. (Not for external publication)

Internal handling

- Protected information should always be marked 'Official Sensitive' whether held in hard or soft copy.

- If the information is received into a shared inbox, we should make a record in the restricted area of SharePoint and delete it from the shared location.

- Electronic information should be held in restricted access SharePoint folders.

- In the unlikely event that it is necessary to hold hard copy records, they should be logged and tracked on the relevant asset register.

- Hard copy records should be held in sealed envelopes within locked storage. Their label should state 'Official Sensitive – access restricted to [list of job titles and names].'

- Do not use the internal mail to pass hard copy protected information.

- Do not refer to protected information within internal correspondence unless it is necessary to do so.

- Consideration should be given to whether the protected information is relevant to the record. If it is, it should be held in line with the retention period. If it is not, it should be destroyed securely.

- Protected information should be destroyed securely and only by using our established confidential waste disposal facilities.

- Case files should be retained for the normal retention period and thereafter destroyed securely.

- If you think an unauthorised disclosure of protected information has or might have occurred, you should inform your line management of the incident, making clear that it involves protected information, as soon as possible.

External handling

- Protected information should not be shared externally unless it is necessary and lawful to do so.

- Correspondence which includes protected information should be clearly marked 'Official Sensitive' however it is sent.

- We should include minimal reference to protected information within correspondence, wherever possible.

- Consideration should be given to the most appropriate method of sending protected information.

- We should ask that any hard copy correspondence sent to us relating to the protected information is double-enveloped, with the outer envelope marked "OFFICIAL SENSITIVE" and the inner envelope marked "OFFICIAL – SENSITIVE – PROTECTED INFORMATION – For the attention of [name]'.

- All protected information sent by post should be sent by Special Delivery.

Back to Top

Annex M. Case acknowledgement template. (Not for external publication)

*YOU MUST ENSURE THIS IS TAILORED TO THE RESPONSE WHERE NECESSARY E.G. TO REQUEST FURTHER INFORMATION. *

Thank you for your correspondence with the Information Commissioner's Office. As it concerns matters relating to a Gender Recognition Certificate (GRC), I wish to outline our procedures for handling such material.

Please note that I also need some further information from you and will be unable to progress the case until I receive your response.

To ensure compliance with the Gender Recognition Act 2004 (GRA), we have developed procedures to limit access to case files where a customer has raised an issue relating to a GRC. Reflecting the potential sensitivity of the information, these go beyond our normal standards.

So, we can begin looking into the matter you have raised, I would be grateful if you would:

• confirm that we can contact [INSERT NAME OF DATA CONTROLLER OR OTHER RELEVANT PARTY] in connection with this matter, and

• provide the name of an appropriate individual within that organisation who we should contact.

On receipt of the above information, we can begin to undertake any necessary investigation. Any correspondence we send to third parties (such as [NAME OF DC]) will include a statement drawing their attention to their duties under s22 of the GRA.

If you want to discuss anything in this letter, or any other details about how we will handle your case, please call me on [DIRECT DIAL NUMBER]

Yours sincerely

NAME
JOB TITLE
Information Commissioner's Office

For information about what we do with personal data see our privacy notice.

Back to Top

Annex N. Enquiry case template. (Not for external publication)

Thank you for your correspondence with the Information Commissioner's Office. As it concerns matters relating to a Gender Recognition Certificate (GRC), I wish to outline our procedures for handling such material.

To ensure compliance with the Gender Recognition Act 2004 (GRA), we have developed procedures to strictly limit access to case files where a customer has raised an issue relating to a GRC. Reflecting the potential sensitivity of the information, these go beyond our normal standards.

Response to enquiry

- If complicated – summarise the question you are answering.
- Give the answer to the question clearly.
- If necessary, add your explanation, signposting if necessary.

If you want to discuss anything in this letter, or any other details about how we will handle your case, please call me on [DIRECT DIAL NUMBER]

Yours sincerely

NAME
JOB TITLE
Information Commissioner's Office

Back to Top

Annex O. Statement drawing attention to the recipient's duties under s22 of the GRA. (Not for external publication)

This case is likely to involve the disclosure of 'protected information' as defined by the Gender Recognition Act 2004 (GRA).

Section 22 of the GRA makes it an offence for anyone who has received such information in an official capacity to disclose that information to an unauthorised individual, subject to limited exceptions. **Importantly, this includes disclosure to other people within your own organisation**.

The scenarios in which the information would be obtained in an official capacity are set out in s22(3) of the GRA. There are also exemptions to the prohibition as set out in s22(4) of the GRA and in the Gender Recognition (Disclosure of Information) (England, Wales, and Northern Ireland) (No.2) Order 2005, and the Gender Recognition (Disclosure of Information) (Scotland) Order 2005.

If you are not clear about your obligations under the GRA, you should take advice from the relevant person in your organisation before disclosing any of the information in this letter.

Back to Top