Policy on the handling of Gender Recognition Certificate cases

November 2020

1. Background

This policy covers the handling of 'protected information' as defined by the Gender Recognition Act 2004 (GRA).

Individuals who:

a) have, or have had, gender dysphoria,
b) have lived fully for the last two years in their acquired gender, and
c) intend to live permanently in their acquired gender,

can apply to the Gender Recognition Panel to be issued with a Gender Recognition Certificate (GRC), under the provisions of the GRA.

Information that enables the identification of an individual who has applied for or obtained a GRC, is given special protection and is known as 'protected information'.

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 the ICO.**

2. Purpose

This policy is intended to help all staff understand and put into practice the statutory requirement to limit the disclosure of protected information relating to a person who has applied for or obtained a GRC. Such information may be provided to the ICO in the following ways:

- As an enquiry for advice and guidance to the ICO
- As a complainant to the ICO.
- As a Personal Data Breach reported to the ICO
- As an existing or prospective ICO employee.

This guidance relates to the first three of these situations. It also considers how to handle a request under the Right of access, from any person who has disclosed that they hold a GRC. Separate guidance on the handling of GRCs from existing or prospective employees has also been prepared for use by Human Resources.

The scenarios in which the information would be obtained in an official capacity are set out in s22(3) of the GRA and include the information being provided in connection with the person's functions as,

(i) a member of the civil service, a constable or holder of another public office, or

(ii) in connection with the functions of a local or public authority or of a voluntary organisation, or

(iii) as an employer or prospective employer of that person with the GRC or in connection with the conduct of business or the supply of professional services.

ICO staff will receive information under category (ii).

The GRA demands that protected information is treated with extra care. This policy will help you to do that.

3. Legal requirements

Present and former members of ICO staff are already prevented from disclosing information received during the course of their work unless it is done with lawful authority as per part 5 section 132 of the Data Protection Act 2018(DPA 2018). An unauthorised disclosure of such information is a criminal offence.

Section 22(1) of the GRA provides additional protection for information relating to a person who has applied for a GRC. Subject to a limited number of exceptions, it is a criminal offence to disclose information obtained in an official capacity which concerns such an application or the person's previous gender.

The exemptions to the prohibition are set out in s22(4) 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. These include disclosure:

- where the person cannot be identified from the information disclosed,
- where the person agrees to the disclosure,
- for the purpose of obtaining legal advice
- in accordance with an order of a court or tribunal,

4. Responsibility

Caseworkers should not feel inhibited in discussing aspects of any GRC-related case with their line manager or other appropriate colleague where it is lawful and necessary to do so. However, any such discussions should meet the reasonable expectations of a person holding a GRC.

GRC-related casework should not be accessible to any member of staff unconnected with the case at any given time.

To assist with this process, the Group Managers (Public Advice & Data Protection Complaints Services) have been designated as GRC points of contact. 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 GRCs.

The Group Manager should in turn appoint a Lead Case Officer who will be a point of contact for their department who may assess, set up, monitor and review potential GRC cases, they should ensure that training is delivered and that case officers and other staff in the department are aware of how to recognise GRC related casework.

The delegated officers are currently:

- Group 1 – [redacted]
- Group 2 – [redacted]
- Group 3 – [redacted]
- Group 4 – [redacted]
- Group 5 – [redacted]
- Group 6 – [redacted]

5. Asset Register

All correspondence relating to Gender Recognition must be kept on in local asset storage and recorded on the asset register.

The asset register in PA is saved in the PA area of SharePoint-shared area-policies and procedures-DP Complaints and Reviews Asset Register. Those responsible for the register are as follows:

Local Information Management Officers (LIMOs):

[redacted]

Local Asset Administrators (LAAs):

Group 1 – [redacted]
Group 2 – [redacted]
Groups 3 & 4 – [redacted]

6. Receiving correspondence

Postal correspondence
If the letter is identified as relating to GRC during the scanning process, the correspondence should be delivered to delegated officers in Public Advice & Complaints department.

The delegated officers will then create a case in the restricted area of SharePoint – as per section 7.

Hard copies of the correspondence should be retained in the PADPC asset register.

Email correspondence
If an email is identified as relating to GRC from the 'icocasework' queue on the ICE case management system, the person processing that queue will download a copy of the correspondence and send it to the Protected cases inbox.

The person processing the 'icocasework' queue will then delete the email from their sent items and contact ICEhelp to have the original email deleted from ICE and the icocasework inbox.

The delegated officers will then create a case in the restricted area of SharePoint – as per section 7.

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

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

Sift
If a GRC sift item is identified in the 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 – as per section 7, download the docs from ICE, add

them to the SharePoint case and then contact ICEhelp to have the sift item deleted from ICE and the icocasework inbox.

NOTE – If an existing case was not identified as relating to GRC, and subsequently opened/dealt with it should be flagged with a Group manager.

ICE cases
GRC cases should not be dealt with on ICE. If a case has been missed at sift, and created in error then deal with them as follows:

If the correspondence was received in the post:

- Request the original document using the document retrieval process.
- Scan the document to your personal drive and follow section 7 (creating a case)

Once the case has been created on SharePoint, the delegated officer will ensure that documents are removed from the existing ICE case, and the case is deleted from ICE.

Delegated officers will need to email ICEhelp requesting the case and correspondence is deleted.

7. CREATING A CASE

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

Delegated officers will identify and confirm that the correspondence/matter relates to the GRA.

Emails

Find the relevant email(s) in the **Protected Cases** inbox.
Save the relevant 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.

Click Save.

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.

ONCE THE EMAIL HAS BEEN UPLOADED IT SHOULD BE REMOVED FROM OFFICER'S DESKTOP.

Postal correspondence

The document(s) should be scanned to the delegated officers email address.

Save the scanned document(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.

Click Save.

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.

- Secondary contact Tick for case changes only.
- Security class: DO NOT CHANGE.

ONCE THE SCANNED DOCUMENT HAS BEEN UPLOADED IT SHOULD BE REMOVED FROM OFFICER'S DESKTOP.

THE POSTAL CORRESPONDENCE SHOULD THEN BE PLACED IN THE ASSET REGISTER.

Complete the GR Case Log

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 caes)

8. Acknowledging the case

The delegated officer should then send an acknowledgement, based on the templates – following email and postal instructions below (sections 8.1 and 8.2).

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, will depend on the way the customer chose to contact us. We should use the same channel that they used, unless they have requested some other arrangement, subject to the general principles in Annex B.

WE SHOULD TAKE NO FURTHER ACTION ON THE CASE – INCLUDING REFERRING IT TO THE RELEVANT CASE OFFICER - UNTIL WE RECEIVE THE CUSTOMER'S RESPONSE.

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".

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 have been allocated the case),and the Group Manager.

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

8.1. Email responses

Open the relevant email from the individual - "DS to ICO (initial) DD/MM/YY"

Click reply **(DO NOT SELECT "REPLY ALL")**

SECURITY CHECK. MAKE SURE THAT THE RESPONSE IS BEING SENT TO THE CORRECT EMAIL ADDRESS.

The email to the individual should be sent from the **Protected cases** NOT an individual email account.

- Change the sender to "**protectedcases**"
  - Select "options"
  - Select "from"
  - Change to casework
  - Remove normal outlook signature.

Draft the response using the templates.

MAKE SURE YOU HAVE COMPLETED ALL OF THE SECTIONS THAT HAVE [SQUARE BRACKETS] BEFORE SENDING.

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 you 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.

ONCE THE EMAIL HAS BEEN UPLOADED IT SHOULD BE REMOVED FROM OFFICER'S DESKTOP.

8.2. Postal responses

Draft the response using the templates found in the appendices.

Templates are saved in the following SharePoint folder:

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) DD/MM/YY"

Upload the relevant email(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.

ONCE THE DOCUMENT HAS BEEN UPLOADED IT SHOULD BE REMOVED FROM OFFICER'S DESKTOP.

9. Enquiry and Complaint cases

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 in section 8.1
- Postal responses should follow the process in section 8.2

When contacting Data Controllers:

- Any correspondence we send to third parties will include a statement drawing their attention to their duties under s22 of the GRA.

You must make sure that the GR Admin log is kept up to date.

10. Referrals to Enforcement

As previously stated, caseworkers should not feel inhibited in discussing aspects of any GRC-related case with their line manager or other appropriate colleague where it is necessary to do so.

However, in general terms, it is likely that the focus of any formal regulatory action we take, will be on the procedures and practices adopted by the data controller for the handling of such 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.

Based on the above, the following processes should be adopted hen handling GRC-related investigations.

If a case is to be referred to Enforcement, you should email the Group Manager, DP Complaints and Reviews, should first 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, the Group Manager in Performance Improvement 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 [redacted]@ico.org.uk (FAO [redacted]).
- 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.

NOTE – Once access is no longer required an email should be sent to [redacted]@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 A, 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.

They will then store the case papers 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 the Group Manager in DP Complaints and Reviews redacted 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 DP Complaints and Reviews 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.

11. Handling GRC-related subject access requests (SARs)

Individuals should be encouraged, where possible, to make subject access requests through the delegated officers responsible for GRC cases.

When it is identified that a SAR relates to a gender recognition case it should be flagged with the Group Manager in Records and Information Management [redacted]

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

- Complete the Request for Access – Restricted SharePoint template and send to [redacted]@ico.org.uk (FAO [redacted]).
- 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.

NOTE – Once access is no longer required an email should be sent to [redacted]@ico.org.uk requesting this is removed.

Acknowledgement

The case handler will acknowledge receipt of the correspondence and advise who will be dealing with it.

They should also ask that any further correspondence relating to the SAR should be sent in accordance with the general principles in Annex A.

Locating information

Existing procedures can be followed to identify who holds information relating to the data subject. However, no reference should be made to the GRC within any internal enquiries seeking to locate records.

Supplying information internally

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

If any of these records are held in hard copy they will need to be kept in secure storage. If they are passed to another team as the case progresses then the physical records should also be passed. They should be logged on the asset register and their movement should be tracked on the register too, making no reference to the GRC content.

The requester may well not require a copy of their GRC or of other information held in relation to it if they already have copies of themselves. Where possible, the IAT should try to agree with the requester the material they want in order to reduce the risks associated with information being duplicated and disclosed.

If the IAT needs to discuss disclosure with colleagues on a case specific basis, wherever possible, only colleagues who have already been involved in the case should be approached.

Responding to the SAR

The IAT will agree with the requestor the means by which the information will be sent to them. Normally this will be by email or by Recorded Delivery. However, consideration should be given to providing the response on encrypted disc. If so, the discs must be created and retained in accordance with the Encrypted Disc Procedure.

12. Information Access Encrypted Disc Procedure

This procedure is to guide the creation, record keeping and retention of encrypted discs. Discs should only be created once the decision to disclose information has been made and it has been decided that the appropriate method to do that is an encrypted disc.

Complete the removable media form –

http://intranet.child.indigo.local/corporate-functions/information-governance/Pages/Security-Manual---removeable-media.aspx

Once this has been authorised, follow the below procedure.

9.1 Creating an encrypted disc

- Save the information for the disc onto your F Drive or desktop. If there is more than one item create a folder and save the files into it. Ensure the folder is named appropriately; you might also want to name each file.

- Call IT Help on [redacted] to make a request for an encrypted disc:

- They may ask you why you need the disc (tell them reason eg for information request or Court Order etc).

- They will ask you for the location of the information to be saved to the disc.

- Ask for two copies of the disc (one will be retained by the ICO) which are given the same password – remind them that the password needs to be a randomly generated combination of characters/numbers (they will generate a password).

9.2 Checking the Encrypted Discs

- The onsite member of the IT help team will give you the encrypted discs and they will email you the password.

- Borrow a DVD/CD drive from IT (they will log the fact that you've borrowed it).

- Plug both the USB connectors into your Wyse box and insert the first of the discs.

- Generally the disc will not open automatically so you will need to go to 'computer' in start and double click on the 'E Drive'.

- The file should have an icon of a padlock next to it (if this icon doesn't show straight away, wait for a couple of minutes as it may not have loaded yet if the files are very large).

- Drag the padlock icon onto your desktop – **NOTE** if you don't move the file to your desktop it cannot be decrypted.

- Double click the padlock icon and you will be presented with a dialogue box asking you to provide the password.

- **You need to be sure that the encryption is working – do not send discs out unless and until you are sure.**

- Test the encryption of the disc by typing in any random letters (not the password) – if the encryption is working it should come up with the message 'wrong passphrase'.

- If the encryption does not work you need to tell the IT help team and ask them to do the task again.

- Type in the correct password and click ok – it may take a while for the file to open depending on the size.

- The file or folder containing files will appear on your desktop – open and check it contains the correct contents.

- Once you are satisfied that the disc contains the correct files and that they are encrypted you should delete the file from your desktop/F: drive.

Note – if you have a copy of the folder/file for the disc on your desktop, you will need to alter the document/folder title before you try to open the file on the disc as the two copies will have the same title and may not open correctly.

9.3 Making a record and retention

- In the IA Team Resources subsite of SharePoint there is an 'IA Team Admin' folder which contains a spreadsheet titled 'Disclosures by Information Access made by disc' which must be completed for each disc sent; ensuring you save the spreadsheet once you have updated it: https://edrm/sites/corp/atii/TeamRes/_layouts/15/DocIdRedir.aspx?ID=CORP-1423627396-9

- Assign the next 'IA' reference number to the disc (e.g. IA-34) and complete the fields on the spreadsheet.

- On the disc retained by the ICO, write the 'IA' reference number of the front of the disc.

- On the disc sleeve (which you can get from Facilities) write the 'IA' reference number on the top right hand corner.

- Store the ICO's copy of the disc in the blue plastic disc container in the Information Access storage (they are stored in 'IA' number order).

- Delete the password from your inbox. It will be retained in the spreadsheet in SharePoint.

9.4 Sending the encrypted disc

- The disc should be sent by recorded or special delivery (depending on the content and circumstance).

- Obtain a small padded envelope and a disc sleeve from Facilities

- The disc which is being sent to the requester should be marked with the relevant reference number. There might be occasions when discs are sent unmarked.

- Check you have the correct address for the recipient and create an address sticker for the envelope.

- Make the recipient aware they should expect an encrypted disc.

- Ensure that a note of the recorded delivery reference number is written on the disc spreadsheet and also on your CMEH case if applicable.

- **Under no circumstances should you send the password with the disc.**

- The password needs to be provided to the recipient separately either by email, phone or by post.

- If applicable, record on the spreadsheet when the recipient has confirmed receipt of the disc.

Annex A – General information handling principles
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.

- Hard copy records should be logged and tracked on the relevant physical 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. You should always pass or collect protected information in person.

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

- Protected information should not be held for any longer than is necessary. Separate 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 relevant to the work. 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.

- Protected information can be sent by email but only if the data subject has been made aware of the risks. They should be told that we do not use encrypted email software and be made aware of the inherent risks associated with email before they make their choice.

- The data subject should always have the option to send information to us in hard copy.

- 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.

- We can also consider whether we should send information via encrypted disc. We will need to check whether this is a practical solution in the circumstances.

- If we do send information this way, you should follow our encrypted disc procedure and record.

Annex B – Case acknowledgement template

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 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.

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.

[EMAIL] We are sending this letter to you by email, because that is how you contacted us. However, you should be aware that we don't use encryption software and there are risks associated with email (as there are with most methods of communication) such as interception. If you wish to continue to correspond by email, please reply directly to this email, taking care not to amend anything in the subject field.

[POST] We are responding via post, because that is how you contact us. You should be aware that when sending us an email, we don't use encryption software and there are risks associated with

email (as there are with most methods of communication) such as interception

When responding to this correspondence by letter, please use two envelopes. The outer envelope should be addressed to this office at the address above. The inner envelope should be marked "OFFICIAL – SENSITIVE – PROTECTED INFORMATION" and "SPG000 FAO [NAME OF CASE WORKER]".

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.

Annex C – Enquiry case template

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're answering
- Give the answer to the question clearly
- If necessary add your explanation

Signposting if necessary

[EMAIL] We are sending this letter to you by email, because that is how you contacted us. However, you should be aware that we don't use encryption software and there are risks associated with email (as there are with most methods of communication) such as interception. If you wish to continue to correspond by email, please reply directly to this email, taking care not to amend anything in the subject field.

[POST] We are responding via post, because that is how you contact us. You should be aware that when sending us an email, we don't use encryption software and there are risks associated with email (as there are with most methods of communication) such as interception

When responding to this correspondence by letter, please use two envelopes. The outer envelope should be addressed to this office at the address above. The inner envelope should be marked "OFFICIAL – SENSITIVE – PROTECTED INFORMATION" and "SPG000 FAO [NAME OF CASE WORKER]".

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

Annex D - statement drawing attention to the recipient's duties under s22 of the GRA

This case is likely 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.

GENDER RECOGNITION CASES
General information handling principles

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 Meridio/Sharepoint folders.

- Hard copy records should be logged and tracked on the relevant physical 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. You should always pass or collect protected information in person.

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

- Protected information should not be held for any longer than is necessary. Separate 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 relevant to the work. 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.

- Protected information can be sent by email but only if the data subject has been made aware of the risks. They should be told that we do not use encrypted email software and be made aware of the inherent risks associated with email before they make their choice.

- The data subject should always have the option to send information to us in hard copy.

- **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**.

- We can also consider whether we should send information via encrypted disc. We will need to check whether this is a practical solution in the circumstances.

- If we do send information this way, you should follow our encrypted disc procedure and record.

SCD and gender identity

Is gender identity special category data?

Information about someone's gender identity isn't automatically special category data, but should always be treated very carefully.

In some cases it might involve special category data, but this depends on the circumstances. For example, if the information also reveals specific details about the person's health status or medical care, or an organisation uses it to make specific inferences about health, that would involve special category data.

If there's no specific information or inference about someone's health (or any other specific category such as sexual orientation or sex life), it isn't special category data. But in many cases information about someone's gender identity is still likely to be particularly sensitive.

Organisations should be careful to think about fairness when handling this sort of information, and we would expect them to treat it with an appropriate level of sensitivity. They could decide to treat it as if it were special category data, to help them make sure they have a good reason for using it and comply with the fairness principle - although this isn't an explicit requirement. This would mean they treat it in a similar way to other similarly sensitive data such as sexual orientation.

They'll also need to think about their equality obligations, to make sure their use of this data is lawful.

You can use our interactive tool to help you identify special category data: Click thinking | Is it special category data?

See also:

What's special category data about health?
What's special category data about sexual orientation?
What's special category data about sex life?

Related keywords: *sensitive data, SCD, gender expression, nonbinary, trans, transgender, gender reassignment, protected characteristics*

Is gender identity special category data?

Information about someone's gender identity isn't automatically special category data, but should always be treated very carefully.

In some cases it might involve special category data, but this depends on the circumstances. For example, if the information also reveals specific details about the person's health status or medical care, or an organisation uses it to make specific inferences about health, that would involve special category data.

If there's no specific information or inference about someone's health (or any other specific category such as sexual orientation or sex life), it isn't special category data. But in many cases information about someone's gender identity is still likely to be particularly sensitive.

Organisations should be careful to think about fairness when handling this sort of information, and we would expect them to treat it with an appropriate level of sensitivity. They could decide to treat it as if it were special category data, to help them make sure they have a good reason for using it and comply with the fairness principle - although this isn't an explicit requirement. This would mean they treat it in a similar way to other similarly sensitive data such as sexual orientation.

They'll also need to think about their equality obligations, to make sure their use of this data is lawful.

You can use our interactive tool to help you identify special category data: Click thinking | Is it special category data?

See also:

What's special category data about health?
What's special category data about sexual orientation?
What's special category data about sex life?

Related keywords: *sensitive data, SCD, gender expression, nonbinary, trans, transgender, gender reassignment, protected characteristics*

Is it special category data?
Is it criminal offence data?
This is an interactive click-through tool for ICO colleagues.

It can help you think about sensitive information, and decide whether it's special category data or criminal offence data.

This tool only looks at the status of the information. If you already know it's special category data and need help navigating the rules and conditions, you can use our separate tool: https://indigoffice.sharepoint.com/sites/Knowledge/SitePages/Click-thinking-SC-conditions.aspx

This tool focuses on the UK GDPR and does not look at use of sensitive information by police or other law enforcement agencies. You may need to consider those issues separately.

There are up to 8 questions in total (depending on the type of information you're looking at). You will then see advice on how the legislation is likely to apply, based on the answers you gave – or whether you need more information (and if so, where you can go).

It should take around 5 minutes to complete. It may take a little longer if you want to look at a combination of potentially sensitive categories.

This tool was last updated on 6 March 2023.

Sensitive categories
1.Does the information have a possible link to any of these topics?
Pick one. If more than one might be relevant, you can come back later to look at the others.

If you're not sure whether there might be a link, or what the category covers, click that category to find out more. We'll take you through some questions to help you decide.

- ○ Racial or ethnic origin
- ○ Political opinions
- ○ Religious or philosophical beliefs
- ○ Trade union membership
- ○ Genetics
- ○ Biometrics
- ○ Health
- ○ Sex life
- ○ Sexual orientation

- (•) Sex or gender identity
- ( ) Criminal offences
- ( ) None of these

Sex or gender identity
This might be information about someone's biological sex.

Or it might be information about someone's gender identity or expression - for example, whether someone is nonbinary or trans.

2.Does the information also clearly reveal something specific about the person's health status or medical treatment?

- ( ) Yes
- ( ) No
- ( ) Not sure
- ( ) No, but there's a possible inference