Workforce Repository and Planning Tool

Information Sharing Gateway (ISG) Manual
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Detail</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Creating a data sharing summary</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>Creating outbound data flows</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>Creating inbound data flows</td>
<td>24</td>
</tr>
<tr>
<td>5</td>
<td>Protected characteristics</td>
<td>34</td>
</tr>
<tr>
<td>6</td>
<td>References</td>
<td>35</td>
</tr>
</tbody>
</table>
Introduction

The Information Sharing Gateway (ISG) has been developed by a sub-group of organisations in the Lancashire & Cumbria IG Group to improve and modernise the administration and risk assessment of information sharing in the public sector. It has been designed by IG specialists for IG specialists, to support their IG reporting on data flows and information sharing (principally to IG Toolkit). The ISG aims to adequately support electronic information sharing across care boundaries in a way that current, paper-based systems cannot and provide assurance that the information being shared, managed and processed will be done so in such a way that is Data Protection Act compliant. It centralises and shares key agreements in a way that is accessible and transparent and has become a key part of the WRaPT process, getting WRaPT projects moving forward quickly as soon as these data sharing agreements are in place. Key benefits of using the ISG include;

- Minimises the risk of breaking the law and consequent enforcement action by the ICO or other regulators
- Gain better public trust by ensuring that legally required safeguards are in place and complied with
- Allows an electronic capture of data sharing agreements which in turn brings all the benefits of an electronic system
- Reduced reputational risk caused by the inappropriate or insecure sharing of personal data

The purpose of this WRaPT ISG manual is to illustrate how a typical data sharing agreement (both inbound and outbound) might display between your organisation and WRaPT and demonstrate how to create them for your organisation in order to begin valuable work with WRaPT.

We recommend that you use this guide to assist in the formation of data sharing agreements but advise that you do not assume that information demonstrated in this guide will accurately represent the data sharing requirements for your organisation’s specific projects with WRaPT.
Creating a data sharing summary

1. **Signing in:** When your organisation has added you to their list of ISG users, you will receive an email inviting you to register on the system. You need to click on the link from the email invitation and register using the email address to which the invitation was sent. If the email address you registered with matches the email address used by your organisation to add you to the users list, you will be automatically verified and able to log straight into the system to view data sharing agreements. For more information on the registration process please click here.

2. Once signed into the ISG site, select the data sharing tab, scroll down to the bottom of the page and select ‘add summary’ to create a new summary or alternatively find your organisation from the data share name list and select the pen icon to edit the summary of the sharing agreement.
3. The first step is to add all the participating organisations into your sharing agreement summary. Please note that the following instructions are based on a standard agreement (example used is Cheshire Pioneer) to share workforce data including some selected protected characteristics. Other agreements may differ based on the information to be shared and other factors.

You can add an organisation in two ways: Click on the 'none selected tab' to pull up a list of organisations with data sharing agreements currently in place. Select an organisation (for example Ash Tree House Medical) and select whether they are providing or receiving data before adding to the agreement:
If an organisation is not in the quick tab list, you can add them by ‘look up’:

Upon selecting lookup, the following box will appear. Use the search fields to find the organisation you would like to add to the data agreement.
4. After adding the organisations involved in the agreement, scroll down and fill in the necessary fields as illustrated below

- **Is an asset linked to the information sharing? If so, please specify:** Not applicable

- **For what purpose is the information being shared?** For workforce planning for the Cheshire Pioneer Programme.

- **What is the legal gateway for sharing?** Schedule 2: The processing is in accordance with the “legitimate interests” condition. Schedule 3: The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

- **What information is being shared?**

  - Personal
  - Personal Sensitive - Low Risk e.g. medical records
  - Personal Sensitive - High Risk e.g. sexual health, children's records
  - Commercial
  - Commercial Sensitive
  - Anonymised / Pseudonymised - Standard
  - Anonymised / Pseudonymised - Non standard
  - Publicly held

- **Select at least one Schedule 2 condition:**

  - Legitimate interest of data controller
To provide a comprehensive view of the cross-economy workforce to better inform workforce redesign throughout the locality by inputting data into reporting and modelling software including "WRaPT" and "Infogr.am".

Year of Birth, Gender, Assignment Number, Ethnic Origin, Religion, Sexual Preference, Disability Status, Contractual Data including WTE, Salary, Role Name, Role Groups, Department, Team Name, Cost Centre and Activity Data (specific to service).
Select a review cycle of between 1 – 3 years (1 is the standard review cycle for WRaPT projects) or a specific review date. If there has been a pre-existing agreement this can be uploaded into the additional files section as shown below. Once the agreement is signed the date signed box can be completed. Click ‘update summary’ to save.
Creating an outbound data flow

1. Within the ISG, select the data sharing tab, find your organisation from the data share name list and select the blue data flow button to create, view and edit data flow agreements.

2. Select add data flow. For demonstration purposes, we have selected Cheshire Pioneer generating the following screen, showing that both inbound and outbound data flows are existing. We will use these flows as a template to demonstrate how your sharing agreement may look.
3. Once directed to the flow page, complete the data flow as demonstrated in the example below

<table>
<thead>
<tr>
<th>Data Flow Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data flow name / identifier:</td>
</tr>
<tr>
<td>Organisation name + Outbound</td>
</tr>
</tbody>
</table>

**Organisations involved in this data flow:**
- CHESHIRE & WIRRAL PARTNERSHIP NHS FOUNDATION TRUST
- CHESHIRE EAST COUNCIL, CW1 1HZ
- Cheshire West and Chester Council, CH1 2NP
- East Cheshire NHS Trust
- MID CHESHIRE HOSPITALS NHS FOUNDATION TRUST, CW1 4
- NHS Eastern Cheshire Clinical Commissioning Group
- NHS South Cheshire Clinical Commissioning Group, C
- NHS Vale Royal Clinical Commissioning Group, CW5 5
- NHS West Cheshire Clinical Commissioning Group, CH
- The Countess of Chester Hospital NHS Foundation Tr
- WRaPT

**What is the direction of the data flow?**
- Outbound - External - To within UK

**What is the frequency of the transfer?**
- Ad-hoc
How many records are being transferred?

Batch - 10,001 - Batch - 100,000
Batch - 100,001 - Batch - 10,000
Batch - 10,001 - Batch - 100,000
Batch - 1,001 - 6,000
Batch - 501 - 1,000
Batch - 501 - 1,000
Batch - 101 - 300
Batch - 301 - 500
Batch - 0 - 10
Transfer - 0 - 10
Transfer - 11 - 50
Transfer - 51 - 100
Transfer - 101 - 300
Transfer - 301 - 500
Transfer - 501 - 1,000
Transfer - 1,001 - 5,000
Transfer - 5,001 - Transfer - 10,000
Transfer - 11,001 - Transfer - 100,000

Transfer Modes and Controls

What is being transferred and how?
- Paper delivered by courier
- Paper hand delivered by staff
- Paper delivered by standard post
- Paper transferred by fax
- Paper transferred by data subject
- Removable media hand delivered by staff
- Removable media delivered by standard post
- Electronic data transferred by email

Controls:
- Password protected document, Email address confirmed

- Secure encrypted email
- Password protected document
- Email address confirmed
- None of the above

Electronic data transferred via automated system to system

Controls:
- Data transferred via a secure network - secure connection / system e.g. https
- Data transferred via a secure network - Via N3 secure connection
- Data transferred via a secure network - Secure encrypted FTP
- Data transferred via a secure network - Medical Interoperable Gateway (MIG)
- Data transferred via a secure network - Published to platform (LPRES)
- View only data via a secure network link - Via N3 secure connection
- View only data via a secure network link - Secure connection / system e.g. https
- View only data via a secure network link - Secure encrypted FTP
- View only data via a secure network link - Medical Interoperable Gateway (MIG)
- View only data via a secure network link - Published to platform (LPRES)
- Access data via a secure network link - Secure connection / system e.g. https
- None of above
Electronic data transferred via manual system transfer (uploaded or downloaded)

- Secure Web Portal
- Via N3 secure connection
- Secure encrypted FTP
- None of the above

Electronic data accessed on-site by staff working for partner organisations

- Honorary Contract
- Works for a 'trusted' organisations
- Confidentiality / non disclosure agreements or similar
- Trained and completed competency test for system
- None of the above

Electronic data transferred via text

Post Transfer Security

Where will the information be stored after transfer?

- Server - personal / shared drive - on organisations premises
- Server - system on organisation premises
- Off site server - UK based
- Off site server - within EEA
- Off site server - outside of EEA
- Secure storage on organisations premises
- Secure storage off organisations premises
- None of the above

How will the information be secured?

- Area accessed by key / keypad / access card
- Password protection
- Smartcard / system password

- None of the above
4. After updating the data flow, select the privacy section of the agreement and follow the example below.

For the purpose of workforce planning for the Cheshire Pioneer Programme.

https://wrapt.org.uk/privacy
Privacy Notice is regularly reviewed and is up to date.

Schedule 2: The processing is in accordance with the "legitimate interests" condition.

Schedule 3: The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

Necessary for records on racial equality

All the data collected for WRaPT has been reviewed by the Information Governance Lead, Lancashire Care NHS FT and has been determined to be adequate, relevant, and necessary.
Assess the technical and organisational measures

Select one or more statements to describe the receiving organisation’s policies, processes and standard operating procedures:
- Assurance in place (e.g. IGT, PSN)
- Clearly defined
- Up-to-date
- Readily available
- Understandable (in plain English) for staff to use
- None of the above

Select one or more statements that describe the receiving organisation’s management of incidents:
- Reviewed including any root cause analysis and action plans
- None of the above

Select one or more statements that describe the receiving organisation’s training for both the system and data:
- Assurance in place (e.g. IGT, PSN)
- Users are aware of their responsibilities when using the asset
- Regularly trained and tested on their understanding
- Understand what to do in the event of a breach or incident
- None of the above

Select one or more statements that describe the receiving organisation’s security of the asset:
- Assurance in place (e.g. IGT, PSN)
- Secure storage (e.g. locked cabinet)
- Secure connection (e.g. https)
- Secure access (e.g. password protected)
- Secure encrypted device (e.g. data stick)
- Managed so only authorised persons can access and access routinely checked
- Audit trail of interactions
- None of the above

Select one or more statements that describe the receiving organisation’s business continuity arrangements:
- Assurance in place (e.g. IGT, PSN)
- Clear business continuity arrangements
- Users are aware of arrangements and appropriately trained
- Regularly reviewed and updated (at least annually)
- None of the above
5. After updating the privacy impact assessment, select the outcome section of the agreement and create a risk assessment using the example below.
<table>
<thead>
<tr>
<th>Description</th>
<th>Controls</th>
<th>Initial rating</th>
<th>Actions</th>
<th>Final rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any personal identifiable or sensitive data must not be sent outside of an organisation in a standard, unencrypted e-mail. The identity of the recipient must also be confirmed.</td>
<td>Controls in place: - Password protected document - Email address confirmed - Secure encrypted email</td>
<td><strong>Low</strong></td>
<td>If an initial rating is considered low, then no further actions to mitigate risks are necessary. This is recorded as <strong>Accept</strong>.</td>
<td>With low risks this can remain marked as <strong>Unset</strong>.</td>
</tr>
<tr>
<td>Email communications between NHS accounts are secure and encrypted but this is not the case for all organisations.</td>
<td></td>
<td></td>
<td>If emails between participating organisations were not secure and encrypted (i.e. some controls are missing) the initial rating should be recorded as <strong>Significant</strong>.</td>
<td></td>
</tr>
<tr>
<td>Automated electronic transfer is taking place over a controlled platform. Security controls should still be implemented and maintained.</td>
<td>Controls in place: - Data transferred via a secure network - secure connection / system e.g. https</td>
<td><strong>Low</strong></td>
<td>If an initial rating is recorded as <strong>Significant</strong> because controls are missing, the action recorded would be <strong>Mitigate</strong> or <strong>Change</strong> with a description of how you intend to reduce the risk recorded. This would allow a final rating of low to be recorded.</td>
<td></td>
</tr>
<tr>
<td>Manual electronic</td>
<td>Controls in place:</td>
<td><strong>Low</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transfer is taking place over a controlled platform. Security controls should still be implemented and maintained.</td>
<td>Controls in place:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Secure Web Portal</td>
<td><strong>Low</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Servers hosted within the UK are bound by UK Law and legislation. You must ensure that the necessary due diligence and checks are made. Make sure access is controlled.</th>
<th>Controls in place:</th>
</tr>
</thead>
</table>
| • Server - personal / shared drive - on organisations premises  
• Server - system on organisation premises  
• Off site server - UK based  
• Secure storage on organisations premises | **Low** |

<table>
<thead>
<tr>
<th>At least one control is in place which enables the information to be accessed securely in the receiving organisation.</th>
<th>Controls in place:</th>
</tr>
</thead>
</table>
| • Key allocation  
• Key issue log  
• System login  
• Log book  
• Area accessed by key / keypad / access card  
• Password protection  
• Smartcard / system password | **Low** |

<table>
<thead>
<tr>
<th>All of the minimum recommended controls are in place relating to the accuracy and completeness of the data.</th>
<th>Controls in place:</th>
</tr>
</thead>
</table>
| • Assurance in place (e.g. IGT, PSN)  
• Staff aware of responsibilities when working with data  
• Clear retention schedules | **Low** |

<p>| All of the minimum Controls in place: | <strong>Low</strong> |</p>
<table>
<thead>
<tr>
<th>recommended controls are in place relating to the retention and disposal of the data.</th>
<th>Controls in place:</th>
<th></th>
</tr>
</thead>
</table>
| • Assurance in place (e.g. IGT, PSN)  
• Policies and procedures which state / define Retention schedules |  |  |

All of the minimum recommended controls are in place relating to subject access requests.  

Controls in place:  

|  |
|---|---|---|
| • Assurance in place (e.g. IGT, PSN)  
• Clearly defined procedures in place for Subject Access Requests for individuals  
• Clearly defined procedures in place to handle rectification and blocking of data |  | Low |

Policies, processes and standard operating procedures for the asset/data are clearly defined, up-to-date, understandable and readily available.  

Controls in place:  

|  |
|---|---|---|
| • Assurance in place (e.g. IGT, PSN)  
• Clearly defined  
• Up-to-date  
• Readily available  
• Understandable (in plain English) for staff to use |  | Low |

Incidents are reviewed appropriately.  

Controls in place:  

|  |
|---|---|---|
| • Reviewed including any root cause analysis and action plans |  | Low |

Users of the data are regularly trained, aware of their responsibilities and understand what to do in  

Controls in place:  

|  |
|---|---|---|
| • Assurance in place (e.g. IGT, PSN)  
• Users are aware of their responsibilities |  | Low |
<table>
<thead>
<tr>
<th>Event / Condition</th>
<th>Controls in Place</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>The asset / data is secure, controlled and interactions recorded.</td>
<td>• Assurance in place (e.g. IGT, PSN)</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>• Secure storage (e.g. locked cabinet)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Secure connection (e.g. https:)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Secure access (e.g. password protected)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Secure encrypted device (e.g. data stick)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Managed so only authorised persons can access and access routinely checked</td>
<td></td>
</tr>
<tr>
<td>Business continuity arrangements are clear, users are aware and trained with</td>
<td>Controls in place:</td>
<td>Low</td>
</tr>
<tr>
<td>regular reviews and updates.</td>
<td>• Assurance in place (e.g. IGT, PSN)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Clear business continuity arrangements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Users are aware of arrangements and appropriately trained</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Regularly reviewed and updated (at least annually)</td>
<td></td>
</tr>
</tbody>
</table>
Disaster recovery arrangements are in place with regular review and testing where appropriate.

Controls in place:

- Assurance in place (e.g. IGT, PSN)
- Regularly reviewed and updated (at least annually)
- Electronic part of a disaster recovery testing regime, regularly tested

---

6. Once your risk log is created, you have the option to list any contacts relevant to the data flow in the agreement. This step is not compulsory and is best used for your reference only.
7. You can also choose to add additional documents to the agreement such as relevant email communications

8. The final part of setting up an outbound data flow agreement is the sign off. Once all the above steps have been completed you can request sign off by the relevant people in your organisation (such as the Caldicott Guardian, Accountable Officer, Information Asset Owner, Data Protection Officer or Senior Information Risk Owner) and by those that the agreement is being shared with. They will receive notification that sign off is required by email.
Creating an inbound data flow

1. Within the ISG, select the data sharing tab, find your organisation from the data share name list and select the blue data flow button to create, view and edit data flow agreements.

2. Select add data flow. For demonstration purposes, we have selected Cheshire Pioneer generating the following screen, showing that both inbound and outbound data flows are existing. We will use these flows as a template to demonstrate how your sharing agreement may look.
3. Once directed to the flow page, complete the data flow as demonstrated in the example below

Data Flow Details

Data flow name / identifier: Organisation name + inbound

Organisations involved in this data flow:
- CHESHIRE & WIRRAL PARTNERSHIP NHS FOUNDATION TRUST
- CHESHIRE EAST COUNCIL, CW11 1HZ
- Cheshire West and Chester Council, CH1 2NP
- East Cheshire NHS Trust
- MID CHESHIRE HOSPITALS NHS FOUNDATION TRUST, CW1 4
- NHS Eastern Cheshire Clinical Commissioning Group
- NHS South Cheshire Clinical Commissioning Group, C
- NHS Vale Royal Clinical Commissioning Group, CW5 5
- NHS West Cheshire Clinical Commissioning Group, CH
- The Countess of Chester Hospital NHS Foundation Tr
- WRaPT

What is the direction of the data flow?
- Inbound - External - From within UK
- Inbound - Internal - On site
- Inbound - Internal - Off site

What is the frequency of the transfer?
- Ad-hoc
How many records are being transferred?

Transfer Modes and Controls

What is being transferred and how?

- Paper delivered by courier
- Paper hand delivered by staff
- Paper delivered by standard post
- Paper transferred by fax
- Paper transferred by data subject
- Removable media hand delivered by staff
- Removable media delivered by standard post
- Electronic data transferred by email

Controls:
- Password protected document, Email address confirmed
- Secure encrypted email
- Password protected document
- Email address confirmed
- None of the above

Electronic data transferred via automated system to system

Controls:
- Data transferred via a secure network - secure connection / system e.g. https
- Data transferred via a secure network - Via N3 secure connection
- Data transferred via a secure network - Medical Interoperable Gateway (MIG)
- Data transferred via a secure network - Published to platform (LPRES)
- View only data via a secure network link - Via N3 secure connection
- View only data via a secure network link - Secure connection / system e.g. https
- View only data via a secure network link - Secure connection / system e.g. Secure FTP
- View only data via a secure network link - Medical Interoperable Gateway (MIG)
- View only data via a secure network link - Published to platform (LPRES)
- Access data via a secure network link - Secure connection / system e.g. https
- None of above
Electronic data transferred via manual system transfer (uploaded or downloaded)

Controls:
- Secure Web Portal
- Via N3 secure connection
- Secure encrypted FTP
- None of the above

Electronic data accessed on-site by staff working for partner organisations

Controls:
- Honorary Contract
- Works for a 'trusted' organisations
- Confidentiality / non disclosure agreements or similar
- Trained and completed competency test for system
- None of the above

Electronic data transferred via text

Post Transfer Security

Where will the information be stored after transfer?
- 4 selected
  - Server - personal / shared drive - on organisations premises
  - Server - system on organisation premises
  - Off site server - UK based
  - Off site server - within EEA
  - Off site server - outside of EEA
  - Secure storage on organisations premises
  - Secure storage off organisations premises
  - None of the above

How will the information be secured?

Area accessed by key / keypad / access card, Password protection, Smartcard / system password

- Area accessed by key / keypad / access card
- Password protection
- Smartcard / system password
- None of the above
4. After updating the data flow, select the privacy section of the agreement and follow the example below

https://wrapt.org.uk/privacy
Privacy Notice is regularly reviewed and is up to date.

Schedule 2: The processing is in accordance with the "legitimate interests" condition.

Schedule 3: The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

Necessary for records on racial equality.

All the data collected for WRaPT has been reviewed by the Information Governance Lead, Lancashire Care NHS FT and has been determined to be adequate, relevant, and necessary.
Assess the technical and organisational measures

Select one or more statements to describe the receiving organisation’s policies, processes and standard operating procedures:

- Assurance in place (e.g. IGT, PSN)
- Clearly defined
- Up-to-date
- Readily available
- Understandable (in plain English) for staff to use

Select one or more statements that describe the receiving organisation’s management of incidents:

- Reviewed including any root cause analysis and action plans

Select one or more statements that describe the receiving organisation’s training for both the system and data:

- Assurance in place (e.g. IGT, PSN)
- Users are aware of their responsibilities when using the asset
- Regularly trained and tested on their understanding
- Understand what to do in the event of a breach or incident

Select one or more statements that describe the receiving organisation’s security of the asset:

- Assurance in place (e.g. IGT, PSN)
- Secure storage (e.g. locked cabinet)
- Secure connection (e.g. https)
- Secure access (e.g. password protected)
- Secure encrypted device (e.g. data stick)
- Managed so only authorised persons can access and access routinely checked
- Audit trail of interactions

Select one or more statements that describe the receiving organisation’s business continuity arrangements:

- Assurance in place (e.g. IGT, PSN)
- Clear business continuity arrangements
- Users are aware of arrangements and appropriately trained
- Regularly reviewed and updated (at least annually)
5. After updating the privacy impact assessment, select the outcome section of the agreement and create a risk assessment. This will be the same as the outbound data flow risk assessment on pages 16-20.
6. Once your risk log is created, you have the option to list any contacts relevant to the data flow in the agreement. This step is not compulsory and is best used for your reference only.

7. You can also choose to add additional documents to the agreement such as relevant email communications.
8. The final part of setting up an inbound data flow agreement is the sign off. Once all the above steps have been completed you can request sign off by the relevant people in your organisation (such as the Caldicott Guardian, Accountable Officer, Information Asset Owner, Data Protection Officer or Senior Information Risk Owner) and by those that the agreement is being shared with. They will receive notification that sign off is required by email.
**Protected Characteristics**

To meet the challenge of providing effective and valuable workforce planning, the WRaPT Team collect and process a range of information relating to a wide variety of organisations across the health and social care economy. Where protected characteristics (Year of Birth, Gender, Ethnic Origin, Religion, Sexual Preference, Disability Status) are being shared with and collected by WRaPT, they are used to create workforce baselines and equality impact assessments which allows workforce planners to ensure that changes do not adversely affect any specific and identifiable group. We take our duty to protect personal information and confidentiality very seriously and are committed to taking all reasonable measures to ensure the confidentiality and security of personal data for which we are responsible. The 8 Principles of The Data Protection Act 1998, as set out below are fully endorsed by the WRaPT Team.

The eight principles require that personal information:

- Shall be processed fairly and lawfully (with all relevant and specific conditions met)
- Shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
- Shall be accurate and, where necessary, kept up to date
- Shall not be kept for longer than is necessary for the specified purpose(s)
- Shall be processed in accordance with the rights of data subjects under the Act
- Should be subject to appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of personal data, or the accidental loss, destruction, or damage to personal data
- Shall not be transferred to a country or territory outside the European economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

WRaPT asks that you provide us with an explicit reason (that aligns with the conditions for processing that are set out in Schedules 2 and 3 of the Data Protection Act) for collecting protected characteristics from your organisation, such as to carry out an equality impact assessment. Without a condition for processing we will not collect personal data.

WRaPT conditions for processing include:

- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals
- The processing is in accordance with the “legitimate interests” condition meaning that shared information is for a legitimate reason, has been balanced against the interests of the individual(s) concerned and is processed fair and lawfully (abiding to The Data Protection Act 1998)
## References

<table>
<thead>
<tr>
<th>Number</th>
<th>Detail</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>ISG Resources</td>
<td><a href="https://www.informationsharinggateway.org.uk/application/resources.aspx">https://www.informationsharinggateway.org.uk/application/resources.aspx</a></td>
</tr>
</tbody>
</table>