Kirklees Council GDPR self-assessment

March 2019

This is the self-assessment model for GDPR compliance arrangements.

For each of the ten sections, please select the description which best describes your service.

By completing this self-assessment, you will:

- identify where you are on the journey to establishing good GDPR compliance practices
- be able to better manage your work by seeing what's left to do
- help the organisation identify our GDPR assurance status

Don’t worry if the descriptions don’t exactly match where your service is – just choose the one that is the best fit. You may feel that some sections are easier to answer than others, but try to answer each one. If you would like to, add in comments in the free text boxes provided on each page.

Glossary:

- General Data Protection Regulation (GDPR)
- Information Asset Owner (IAO): this is your Service Director
- Central Archive: the archive facility for all council paper records

The self-assessment should be completed online using the invite link you will have received.

This printable version can be used first if you wish, to help you talk through your service responses as a group.

If you chose to record results for your service on this paper version, you will need to transfer your answers into the online self-assessment form once you have finished.

You can tick the description below that is the best fit for your service: ✓

1. Governance

Not started

- We have not made any changes to our procedures, begun our data flow mapping, implemented our Information Asset Owner (IAO) responsibilities or raised GDPR related risks. ○

Planning

- We are becoming aware of GDPR requirements and are identifying the processes which include personal data. We are starting our data flow mapping in key teams. ○

Developing

- We have begun service-wide data flow mapping. We are still to look at implementing IAO responsibilities and have not identified any GDPR service risks. ○

Implementing

- Data flow mapping has identified a range of areas we need to focus on. We have begun to implement IAO responsibilities. GDPR risks is an agenda item at all service management team meetings. ○

Established way of working

- We regularly review our data flow maps. Individuals are carrying out their tasks and reporting to the managers delegated these responsibilities by the IAO. GDPR risks are discussed at all operational team meetings. ○

You can use this space to specify any areas where you need help:

You can tick the description below that is the best fit for your service:

2. Assurance

Not started

- We have not thought about how we should have an appropriate method of ensuring GDPR compliance across the service and with our contractors. ○

Planning

- We are thinking about what we need to do to ensure GDPR compliance within teams and with our contractors. ○

Developing

- We are starting to identify the requirements for our GDPR compliance and what we would need to do to ensure our teams and contractors are able to achieve these requirements. ○

Implementing

- We are implementing regular checks across the service to ensure that our GDPR compliance requirements are being met and are starting to work with our contractors on their GDPR arrangements. ○

Established way of working

- We routinely check each team's GDPR compliance arrangements against the service requirements and are contract managing GDPR compliance with all our contractors to ensure robust GDPR assurance. ○

You can use this space to specify any areas where you need help:

You can tick the description below that is the best fit for your service: ✓

3. Third party management

Not started

- We do not have a list of our data processors, have not adjusted our contracts to include new GDPR clauses, have not identified where we share information with other organisations or have any contract management procedures around processing of personal data. ○

Planning

- We are beginning to identify which contractors process personal data on our behalf. We are thinking about where we share our data with other organisations through our data flow mapping. ○

Developing

- We are identifying all contractors who process personal data on our behalf. We have identified our data processing contracts and are adjusting these. We have identified where we share data with other organisations through our data flow mapping. We are thinking about how we could support our commissioned services to be GDPR compliant. ○

Implementing

- We have a list of third parties who process personal data on our behalf. We have adjusted our contracts for GDPR compliance. We are setting up information sharing agreements for all organisations we share data with. We are creating guidance to ensure robust contract management for GDPR compliance. ○

Established way of working

- We regularly review our register of data processors. All data processing contracts are identified in the procurement process and appropriate clauses included within the final contracts. We have all information sharing arrangements identified in our data flow maps set up with information sharing agreements which are regularly reviewed. We have strong contract management support procedures for all commissioned services, including guidance around contracts containing the processing of personal data. ○

You can use this space to specify any areas where you need help:

You can tick the description below that is the best fit for your service: ✓

4. Data collection and use

Not started

- We have not started our data flow mapping. We do not have a service level Privacy Notice, or team/project level Privacy Notices. We are not clear on the lawful basis we are using to process personal data. We have not created any entries into the Information Asset Register. ○

Planning

- We are planning how we will roll out data flow mapping for the service. We are thinking about what we need to have in a service Privacy Notice and are planning the process we need to have for teams to create their privacy notices. We are planning how we can identify our Information Assets. ○

Developing

- We are rolling out data flow mapping for each team. We have a service Privacy Notice and are thinking about where we will need Privacy Notices for our teams/projects. We know that we need to identify the lawful basis for processing personal data. We are developing a way to manage consent processes. We are identifying our Information Assets and starting to enter them onto the Information Asset Register. ○

Implementing

- We have completed data flow maps for each team. We have our service and team/project Privacy Notices published on the council's Privacy webpage. We have identified the lawful basis for processing all of the personal data we collect and hold. We have identified all of the Service Information Assets. ○

Established way of working

- Data Flow Mapping is complete and reviewed regularly in all teams. Service and team/project Privacy Notices are regularly updated and published on the council's Privacy webpage. The lawful basis for processing personal data is fully understood in each case. The service has an effective method of managing consent. All information assets, created and used by the service are entries on the council’s Information Asset Register. ○

You can use this space to specify any areas where you need help:

You can tick the description below that is the best fit for your service: ✓

5. Retention and disposal

Not started

- We do not have a retention schedule. We do not often destroy records or if records are destroyed, we don't record this. We do not store any records at the Central Archive and we are not sure of what records we hold or where they are. ○

Planning

- We are discussing retention of records and how we are best rolling this out to the service. We are identifying all of the records we hold and which ones we should keep and which we should destroy. ○

Developing

- We are developing a service Retention Schedule and teams are looking at what records they need to retain. We are looking at the process we are using for record destruction. We are investigating the location of all of our information assets and deciding which need to be moved to the Central Archive. ○

Implementing

- We have a service retention schedule and our teams are developing their own retention schedules if this is appropriate. We have identified all of our information assets and know where they are all located (hard copy and electronic versions). We are in the process of destroying the information assets we don't need to retain. We are updating the Information Asset Register with the information assets we have identified. ○

Established way of working

- Teams have reviewed their retention schedules for all council records. The service has created a service Retention schedule, communicated it to all our staff and published it online. The service has established and implemented a process for managing and monitoring retention periods. The service has implemented a process for the destruction of personal data when no longer required and has procedures in place to regularly update the Information Asset Register and Disposal Log accordingly. The service stores data appropriately in the Central Archive and updates the Information Asset Register accordingly. ○

You can use this space to specify any areas where you need help:

You can tick the description below that is the best fit for your service: ✓

6. Individuals' rights

Not started

- We don't really understand the rights of individuals which have been introduced with GDPR. ○

Planning

- We have looked at the rights introduced by GDPR and are discussing these with teams as appropriate. We are planning how we should respond to a request if it comes in. ○

Developing

- We understand the scope of individuals' rights and will deal with any requests which come in but we find it difficult to meet the GDPR timescales. ○

Implementing

- We have thought about how we could respond to requests from individuals to exercise their rights and are setting up procedures within the service to manage these requests and check GDPR timescales will be met. ○

Established way of working

- We have implemented cross-service procedures to respond to individual rights requests and have a monitoring process in place to ensure GDPR timescales are achieved each time. ○

You can use this space to specify any areas where you need help:

You can tick the description below that is the best fit for your service: ✓

7. Information security

Not started

- We have not considered any specific information security controls. We have not identified any security risks associated with the data we hold. ○

Planning

- We are planning our service incident response plan and have discussed security controls at management team meetings. ○

Developing

- We know that we need to report incidents centrally, using the online reporting form and are communicating this to our staff. We are reviewing our service incident response plan and have discussed security controls at our operational team meetings. We are reviewing our business continuity plan and will consider what GDPR compliance requirements are needed. ○

Implementing

- We have created a service incident response process and are starting to communicate this process to our staff. We are identifying the security controls which are required and are creating security plan. We are identifying any data integrity controls. We are entering GDPR compliance requirements into our business continuity plan. ○

Established way of working

- We have implemented a service incident response process and all staff understand what needs to happen if they become aware of an information security incident. We have implemented service security controls for the building and our data storage areas and have communicated these to all staff. We have documented current data integrity controls and identified and reported any gaps. We annually update our business continuity plan with GDPR compliance requirements. ○

You can use this space to specify any areas where you need help:

You can tick the description below that is the best fit for your service: ✓

8. Systems and technology

Not started

- We have not identified where any gaps exist within our systems relating to GDPR compliance. ○

Planning

- We are identifying all of the systems we have and use within the service. We are looking into which of these require the use of personal data. ○

Developing

- We are investigating what changes we require to our systems or what new approaches we may need to establish which will enable our systems to be fully GDPR compliant. ○

Implementing

- We are implementing any changes to our systems, changes which are required to the systems we use or we have developed new approaches to ensure all of the systems and technology we use is fully GDPR compliant. ○

Established way of working

- We annually review any changes to our systems, changes required to the systems we use or developed new approaches to ensure all of the systems and technology we use is fully GDPR compliant. ○

You can use this space to specify any areas where you need help:

You can tick the description below that is the best fit for your service: ✓

9. Training and awareness

Not started

- We are aware of the available training but have not done any further investigation. ○

Planning

- We have asked all staff to complete the GDPR training. ○

Developing

- All staff have completed the GDPR training. We are looking into how we should roll training out to volunteers or contractors. ○

Implementing

- We have made sure all our staff have completed the GDPR training and are encouraging volunteers and contractors to complete this. We are investigating which teams need further specific training and will commission this from IG as required. ○

Established way of working

- All of our staff, volunteers and contractors have completed GDPR training and any associated specific training. This has all been logged as complete within MiPodXtra. Privacy by Design training has been commissioned from the IG Team. ○

You can use this space to specify any areas where you need help:

You can tick the description below that is the best fit for your service: ✓

10. Staff data

Not started

- We are aware of the need to have personal data deleted if it is not implemented. ○

Planning

- We are encouraging our staff to read the council's Employee Privacy Notice. ○

Developing

- We have encouraged our staff to read the council's Employee Privacy Notice. We have asked our managers to investigate whether they have any personnel data they do not need to keep. ○

Implementing

- All our staff have read the council's Employee Privacy Notice. Managers are deleting historic staff data relating to employees in line with the People Services Retention Schedule. ○

Established way of working

- All of our staff have read the council's Employee Privacy Notice and we have discussed it at team meetings to ensure all questions have been answered. All staff have deleted all employee personal data in line with the People Services Retention Schedules and we continue to ensure this is carried out regularly. ○

You can use this space to specify any areas where you need help:

Please tell us your name:

____

Please select your Information Asset Owner:

This will usually be your Service Director

- ❑ Elaine McShane
- ❑ Jo-Anne Sanders
- ❑ Helen Sevens
- ❑ Sue Richards
- ❑ Amanda Evans
- ❑ Naz Parkar
- ❑ Joanne Bartholomew
- ❑ Rachel Spencer-Henshall
- ❑ Julie Muscroft
- ❑ Eamonn Croston

Finally, please tell us which service you work in:

____

If you have chosen to record results for your service using this paper version of the self-assessment, you now need to transfer your answers into the online self-assessment form.