

## DUMMY INFORMATION - DEMO PURPOSES ONLY



Please update the form for your department and return to [information.officer@cityoflondon.gov.uk](mailto:information.officer@cityoflondon.gov.uk) by the 7th of the reporting period.

| GDPR Departmental Self-Audit Monitor                                                                                                                                                                                                                                                         | Sub Dept.1                                                                            | Sub Dept.2 | Sub Dept.3 | Sub Dept.4 | Exceptions |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|------------|------------|------------|------------|
| <b>Department :</b><br><b>Reporting Period: October 2018</b>                                                                                                                                                                                                                                 |                                                                                       |            |            |            |            |
| <b>Compliance Action</b>                                                                                                                                                                                                                                                                     | Enter a number between 0-3 using the definitions below against each compliance action |            |            |            |            |
| <b>GDPR Risks</b><br>Key risks to compliance understood and notified to Compliance team. i.e 3rd party contracts not GDPR compliant, no record of consent from the data subject, no records retention schedule in place, processes do not comply with data subjects rights.                  | 1                                                                                     | 3          | 2          | 1          |            |
| <b>Awareness - Communication &amp; Guidance</b>                                                                                                                                                                                                                                              |                                                                                       |            |            |            |            |
| Any job-specific training needs are identified and being managed                                                                                                                                                                                                                             | 2                                                                                     | 1          | 1          | 3          |            |
| All staff are aware of the GDPR issues and queries process                                                                                                                                                                                                                                   | 1                                                                                     | 1          | 0          | 3          |            |
| <b>ROPA and Records Management</b>                                                                                                                                                                                                                                                           |                                                                                       |            |            |            |            |
| Records Retention Schedule in place                                                                                                                                                                                                                                                          | 1                                                                                     | 3          | 3          | 1          |            |
| Process for updating Retention Schedule is in place                                                                                                                                                                                                                                          | 2                                                                                     | 2          | 3          | 1          |            |
| ROPA in place                                                                                                                                                                                                                                                                                | 3                                                                                     | 1          | 3          | 3          |            |
| Process for updating ROPA is in place                                                                                                                                                                                                                                                        | 3                                                                                     | 1          | 2          | 1          |            |
| <b>Communicating privacy information</b>                                                                                                                                                                                                                                                     |                                                                                       |            |            |            |            |
| Process for updating and communicating privacy notices (how the City of London Corporation as a data controller collects and uses personal information) is in place                                                                                                                          | 3                                                                                     | 2          | 2          | 2          |            |
| <b>Lawful basis for processing personal data - consent</b>                                                                                                                                                                                                                                   |                                                                                       |            |            |            |            |
| Records are kept for where consent has been received from the data subject                                                                                                                                                                                                                   | 3                                                                                     | 2          | 1          | 1          |            |
| <b>Contracts</b>                                                                                                                                                                                                                                                                             |                                                                                       |            |            |            |            |
| There are written agreements in place with all third party service providers and processors, including those who process personal data on behalf of the City of London Corporation as a data controller, that ensure the personal data that they access and process is protected and secure. | 3                                                                                     | 0          | 0          | 2          |            |
| <b>Data Subjects Rights</b>                                                                                                                                                                                                                                                                  |                                                                                       |            |            |            |            |
| All relevant staff are aware of the process for an individuals' requests to access their personal data (SAR , Right to Access )                                                                                                                                                              | 2                                                                                     | 2          | 3          | 3          |            |
| Guidance is in place to respond to individuals' other rights<br>Right to rectification<br>Right to Erasure<br>Right to Restriction<br>Right to Data Portability<br>Right to Object<br>Right to Object to Automated Decision Making / Profiling                                               | 1                                                                                     | 2          | 3          | 2          |            |

|                                                                                                                                                                                                                                                                        |   |   |   |   |                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---|----------------------------------------------------------------------------|
| Guidelines for processing children's data are in place                                                                                                                                                                                                                 | 0 | 0 | 0 | 0 |                                                                            |
| <b>Data Protection</b>                                                                                                                                                                                                                                                 |   |   |   |   |                                                                            |
| All staff have read the CoL Data Protection Policy 2018                                                                                                                                                                                                                | 1 | 1 | 1 | 1 |                                                                            |
| All staff are aware of the Data Protection Impact Assessment procedure and guidance                                                                                                                                                                                    | 1 | 1 | 1 | 1 |                                                                            |
| All staff are aware of the process for identifying and reporting a Data Protection breach                                                                                                                                                                              | 2 | 2 | 3 | 3 |                                                                            |
| Electronic communications conform to PECR (Privacy and Electronic Communications Regulations) i.e marketing by phone, email, text or fax; use of cookies or a similar technology on the CoL website; or compiling a telephone directory (or a similar public directory | 0 | 0 | 0 | 1 |                                                                            |
| Guidance in place for transferring data securely outside of the EU                                                                                                                                                                                                     | 2 | 3 | 2 | 1 |                                                                            |
| Guidance in place for transferring data securely between CoL and 3rd parties                                                                                                                                                                                           | 3 | 3 | 2 | 0 |                                                                            |
| All staff have read the CoL Information Security Policy and the Security Policy - People                                                                                                                                                                               | 0 | 0 | 0 | 0 | Note: This policy document and guidance will be formally issued very soon. |
|                                                                                                                                                                                                                                                                        |   |   |   |   |                                                                            |

|                           |                                         |    |    |    |
|---------------------------|-----------------------------------------|----|----|----|
|                           | <b>DO NOT ENTER DATA IN THESE CELLS</b> |    |    |    |
| Count                     | D1                                      | D2 | D3 | D4 |
| 3 - Fully implemented     | 30                                      | 20 | 30 | 25 |
| 2 - Partially implemented | 25                                      | 30 | 25 | 15 |
| 1- Not yet implemented    | 30                                      | 30 | 20 | 45 |
| 0- Not applicable         | 15                                      | 20 | 25 | 15 |

#### Supplementary Notes

These questions and definitions are largely taken from the ICO GDPR self-assessment tool

#### Compliance Graph

