THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Operational

Data Protection and managing information

Guidance for staff

Article 30 of the General Data Protection Regulation (GDPR) requires that we keep records of the personal data we hold. We also have a requirement to keep it secure (Data Protection principle 6), only collect what we need (principle 3), keep it accurate (principle 4) and get rid of it when we no longer need it (principle 5). This guidance covers how the School needs to manage information to comply with these requirements.

Article 30 – records of processing activities

Article 30 of the GDPR requires that the School keep records relating to personal data that we process. The information we need to include is:

1. the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
2. the purposes of the processing;
3. a description of the categories of data subjects and of the categories of personal data;
4. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
5. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
6. where possible, the envisaged time limits for erasure of the different categories of data;
7. where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

The School has chosen to cover this requirement using an Information Asset Register (IAR). The initial data was collected in 2017-18 and will be subject to review[1]. The Information Asset and Records Management Policy lists

[1] At the time of writing, the review has been suspended due to the work required for Covid-19 preparations.

the data we are collecting to meet the requirements of Article 30 for business personal data[2]. For example, condition 6 above maps to Retention.

Business units should keep their IAR up to date. Contact the Data Protection Officer via glpd.info.rights@lse.ac.uk if you have any queries related to this.

Keeping personal data secure

Part of managing personal data is keeping it secure. The main points to consider are:

- keeping data in secure areas e.g your OneDrive, SharePoint, Teams, secure drives
- always using encryption in transit and where necessary at rest
- sharing data only with people who need it and ensuring that they have access only to the data they need. Keep in mind there are:
    - three types of data classification - public, restricted, and confidential and
    - three access permissions levels - need to know, least privileged, and role-based access.
- use the secure file transfer system Filedrop for sharing large files over 39GB securely
- use a virtual private network (VPN) like Pulse or the remote desktop (desktop.lse.ac.uk) when accessing external data that requires secure access like some research data
- keeping paper based data locked away when you are not working on it
- ensuring that family, friends and other people cannot access the personal data on your device e.g. use different accounts for different family members
- if using a third party provider to collect or store personal data, you will need to fill out a cloud assurance questionnaire. Contact dts.cybersecurity.and.risk@lse.ac.uk for the form.

Only collect what you need

Consider carefully if you need personal data before you collect it. Whatever you collect, you will have to manage. The less you collect, the less management you have to do.

Keeping data accurate

The fourth data protection principle requires that personal data is kept accurate. Part of managing personal data is that you review personal data, in particular, contact data on a regular basis to make sure it is up to date. Build into your processes a review process for contact data and/or other personal data which has the potential to change regularly.

Managing retention of data

Information has a life cycle, where it is created or collected, used and then disposed of. A small amount of the business personal data we create will be of historical importance, but most can be deleted when we no longer need it. Electronic data should be deleted from recycled bins and backups when we no longer need to retain it. Paper based data should be destroyed via the School's secure destruction service if in the office or shredded or redacted via stamping or black marker pen (cover the personal data on both sides of a document) if at home.

Anonymisation and pseudonymisation

One way not to be subject to the above is to anonymise or pseudonymise data before saving it. Anonymisation completely removes any identifiable data while pseudonymising it removes enough to make it harder for a third

[2] Work is being undertaken by the Research Data Management Working Group to collect the data required for research datasets.

party to re-identify the data. While normal records management rules still apply e.g retention management, file labelling, data protection legislation will not.

Guidelines on anonymisation and pseudonymisation are available for both academic researchers and general School business. As a general rule, take out names and obvious identifiers before displaying data. This is particularly important for special categories data like health data.

Review schedule

Review interval	Next review due by	Next review start
3 years	31/10/2023	01/10/2023

Version history

Version	Date	Approved by	Notes
1	20/10/2020	IGMB	

Links

Reference	Link

Contacts

Position	Name	Email	Notes
Information and Records Manager	Rachael Maguire	r.e.maguire@lse.ac.uk	

Communications and Training

Will this document be publicised through Internal Communications?	**~~Yes~~/ No**
Will training needs arise from this policy	**~~Yes~~/ No**
If Yes, please give details	