Operational

Blogging and Data Protection

Guidance for staff

This guidance takes you through what you need to do to comply with the General Data Protection Regulation (GDPR) and other data protection legislation while blogging.

Why do you need to comply

While the posts you write may or may not contain personal data, there is personal data created and stored as you blog. This includes things like:

- Blog post comments data (name, email, IP)
- Traffic stats plugins/tools such as Google Analytics
- 3rd party hosted services such as Jetpack, Bloglovin' and Disqus
- Email signup forms such as Mailchimp or FeedBurner
- Contact forms
- Drafts of blogposts, possibly containing personal data you don't end up publishing. Note, if you have not published a draft or have used the content you are going to in another post, you should delete any draft older than 6 months.
- Issues relating to the location of your web host. E.g. data is transferred to servers outside the EU.

You may not be using all of these, but it is likely you'll be using at least one or two. If you are, you are processing personal data and this means you need to be compliant with the GDPR, the Data Protection Act 2018 and any other data protection legislation.

What does compliant mean?

To be compliant means the following:

1. You have a lawful basis for processing the data, likely legitimate interests (use where you can) or consent (use only when legitimate interests doesn't apply).
    - Legitimate interests will cover blog comment data and analytics.
    - Consent will cover signing up to receive notifications of blog posts or to mailing lists. It can be withdrawn at any time, so you need to be certain that you can stop notifications or mailings as soon as possible after you have been told that the individual no longer wishes to receive them. It is best if they can inform you via the page they entered their details that they are withdrawing consent. If that is not possible, have a prominent email address on that page that they can use to contact you.
2. You have recorded that you are keeping this data as part of your business unit's Information Asset Register.
3. You are transparent about any third party services you are using e.g. MailChimp to collect data e.g. if the data entered on an online form will be stored by a third party, mention this at the top of the form. This is particularly important for third party services outside the EEA. US companies covered by the privacy shield should be OK to use. If you are uncertain, contact Rachael Maguire, the Data Protection Officer r.e.maguire@lse.ac.uk, who can check a service for compliance.
4. You are transparent about the licences you are applying to your own blog or which licences you are relying on to report content from other sources, e.g. Creative Commons.
5. You deal with easy requests to correct information e.g. a misspelt name.
6. You forward any requests for information held to the Information Rights team (using glpd.info.rights@lse.ac.uk) and provide any information you hold to them within the one month response limit.
7. You link to the School's privacy policy: https://www.lse.ac.uk/lse-information/privacy-policy somewhere on your blog.
8. You keep data secure. If at any point you or a third party discover that personal data relating to personal data processed for your blog has been breached, report this to glpd.info.rights@lse.ac.uk.
9. If you keep a list e.g. in Excel, of contributors, you are keeping this list secure. You could keep this data for as long as the blog is running, but delete it once you have closed down a blog.

Using personal data in a blog post

Aside from the data listed above, you may also be using interviews with or profiles of people as blog content. As long as that individual is aware that you are including their interview/profile on the blog, you should be fine. If you are using anonymised interviews, make sure they are properly anonymised. That is, don't just take out a name, look for other identifying information e.g 'as a Glaswegian' or 'living in Aylesbury'.

Also, ensure that any photos you use you have permission to and can provide proof of that permission. You may still have to take them down on request. This can get tricky with photographs taken in public. Some countries like the UK take the line that photographs taken in public places are legitimate, other countries do not. A list of what is allowed by different countries is here: https://commons.wikimedia.org/wiki/Commons:Photographs_of_identifiable_people. Note the table in this link also gives the copyright position in different countries regarding taking, publishing and commercial use of pictures.

Review schedule

Review interval	Next review due by	Next review start
3 years	28/02/2025	1/02/2025

Version history

Version	Date	Approved by	Notes
1	05/02/2019	Information Governance Committee	
1.1	11/03/22	Information Governance Management Board	Reviewed with no changes required

Contacts

Position	Name	Email	Notes
Data Protection Officer	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	