

LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE (LSE)

DATA-SHARING AGREEMENT FOR USE IN COMPLIANCE WITH PREVENT STATUTORY DUTY UNDER COUNTER-TERRORISM AND SECURITY ACT 2015 - April 2018 version

Purpose

1. The purpose of this agreement is to ensure that LSE complies with its legal duties under the Counter-Terrorism and Security Act 2015 (“the Act”) and associated Prevent duty statutory guidance (“the Purpose”), in respect of data sharing about individuals thought to be at risk of radicalisation. As such, this agreement seeks to ensure that LSE only shares data with the third-party signatory where it is deemed to be appropriate and necessary for the purposes of meeting the School’s statutory obligations. The aim of sharing data with the third-party signatory is to contribute towards the process of supporting individuals who may be at risk of being drawn into terrorism.

Organisations involved

2. This agreement is between LSE and the third-party signatory specified at the end of this agreement. In principle, the third-party signatory will be one of the organisations and individuals specified in Section 37 of the Act (“Membership and proceedings of panels”). However, if necessary, the third-party signatory may also be one of the organisations and individuals specified in Schedule 7 of the Act (“Partners of local panels”).

Principles of data-sharing

3. The data to be shared may comprise personal data and/or any other data relevant to LSE’s compliance with the Prevent duty.
4. LSE will only share data for this Purpose in accordance with the principles enshrined in the statutory guidance and set out at Annex A to this Agreement. For example, there is a need to ensure that any proposed instance of sharing data is a necessary and proportionate response to the risk identified.

Legal basis for sharing

5. The legal basis for sharing data as specified above is by virtue of section 26 of the Act. LSE is a 'specified authority' as defined in Schedule 6 of the Act.

Internal procedure

6. The LSE Prevent Group, in consultation as necessary with other members of the LSE community, will recommend to the LSE Director or, in his or her absence, a Pro-Director deputising for the Director, whether data needs to be shared with the third-party signatory under this agreement. A written risk assessment will form part of the recommendation. No personal data may be shared for this Purpose without the express approval of the LSE Director, or in his or her absence a Pro-Director deputising for the Director.
7. The Head of Legal Team in the Secretary’s Division will advise on any questions in relation to the data to be shared concerning compliance with the Data Protection Act 1998 or other relevant legislation, and if necessary, will seek advice from LSE’s external legal advisers.

Consent

8. Wherever appropriate and insofar as it is possible, the consent of any individual whose personal data is to be shared will be sought prior to the sharing of the data.

Security

9. Data shared for this purpose may be transmitted by hard copy or encrypted email¹; emails will be sent with a sensitivity setting of 'Confidential' and hard copy will be similarly marked.
10. LSE will require the third-party signatory, at all times, to treat the data received with an appropriate degree of confidentiality.

Record management

11. A record of each sharing event will include the date, the name of the organisation with which the data have been shared and details of the transaction, and will be securely retained by the LSE Risk and Compliance Unit for one year after the date on which the data was shared or for such other period as may be required or recommended by the regulatory authority, the Office for Students.

Validity

12. This agreement will remain in force for one year from date of signature, and may by mutual agreement between the signatory organisations be renewed thereafter for an agreed period, with any necessary amendments.

Compliance

13. This agreement was examined by the LSE General Data Protection Regulation (GDPR) Project Team in April 2018 and, with minor changes, judged compliant with the GDPR when it comes into force on 25 May 2018.

Signatory organisation	London School of Economics and Political Science
Name	Louise Nadal
Position	School Secretary
Signature	
Date	

Signatory organisation	
Name	
Position	
Signature	
Date	

¹ .docx and .xlsx files may be adequately encrypted by password-protecting them.

ANNEX A

PRINCIPLES FOR SHARING OF DATA

The following is an extract from *Revised Prevent Duty Guidance for England and Wales: Guidance for specified authorities in England and Wales on the duty in the Counter-Terrorism and Security Act 2015 to have due regard to the need to prevent people from being drawn into terrorism*, originally issued on 12 March 2015 and revised on 16 July 2015.

21. The *Prevent* programme must not involve any covert activity against people or communities. But specified authorities may need to share personal information to ensure, for example, that a person at risk of radicalisation is given appropriate support (for example on the Channel programme). Information sharing must be assessed on a case-by-case basis and is governed by legislation. To ensure the rights of individuals are fully protected, it is important that information sharing agreements are in place at a local level. When considering sharing personal information, the specified authority should take account of the following:

- necessity and proportionality: personal information should only be shared where it is strictly necessary to the intended outcome and proportionate to it. Key to determining the necessity and proportionality of sharing information will be the professional judgement of the risks to an individual or the public;
- consent: wherever possible the consent of the person concerned should be obtained before sharing any information about them;
- power to share: the sharing of data by public sector bodies requires the existence of a power to do so, in addition to satisfying the requirements of the Data Protection Act 1998 and the Human Rights Act 1998;
- Data Protection Act and the Common Law Duty of Confidentiality: in engaging with non-public bodies, the specified authority should ensure that they are aware of their own responsibilities under the Data Protection Act and any confidentiality obligations that exist.