



LEGAL SERVICES
BOARD

Legal Services Board
The Rookery
2 Dyott Street
London WC1A 1DE

www.legalservicesboard.org.uk

Fol request (Ref: 20191124/01)

Thank you for your request for information about the use of personal devices at the Legal Services Board.

I confirm that LSB holds the information that you have requested.

1. Does Legal Services Board allow staff to use their own devices to access work email? Please answer Yes or No.

Yes

2. Does Legal Services Board allow staff to use their own devices for any other work-related activities? Please answer Yes or No.

Yes

3. If you answered yes to question 2 please provide a list of the types of systems that staff can access from personally owned devices?

Office 365 suite, HR system, finance system

4. Does Legal Services Board have a policy that covers BYOD or the use of personal devices at work? Please answer Yes or No.

Yes

5. If you answered yes to question 4 please could you provide a copy of your policy that covers BYOD or personal device usage at work?

Please find this enclosed. We will be reviewing this policy with a view to updating it if required.

If you are dissatisfied with this response to your request for information, you have the right to ask for an internal review / to submit a complaint (see [LSB's Freedom of information – Complaints procedure](#)).

If you are dissatisfied with the outcome of your complaint, you may refer the matter to the Information Commissioner for a decision. Please be aware that the Commissioner will be unlikely to make a decision until you have been through our internal complaints procedure first. You can write to the Commissioner at:

FOI/EIR Complaints Resolution
Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

The reference for your request, which should be quoted in all correspondence, is:
20191124/01.

Yours sincerely

Enclosure: LSB Colleague Handbook of Policies: Email and Internet Use

8. Use of laptops and personal devices

There are a limited numbers of LSB laptops and Blackberry handsets available for colleagues' use, to enable home working (with remote access to standard LSB systems). Priority for use of LSB laptops will be given to those colleagues who have a contractual agreement to work from home and request one. Colleagues are also permitted to use their own equipment (PC, laptop or Mac) to access LSB systems, subject to the conditions set out in paragraphs 8.4 and 8.5 below, and any supplementary guidance provided. No data can be stored on a remote device when connected to the LSB system as users are effectively 'working on the server' and files never leave the LSB server. (This does not apply to any attachments that may be sent to personal email accounts).

In relation to the use of both LSB issued laptops, Blackberry handsets and own devices for work purposes, colleagues should ensure that they adhere to confidentiality, integrity and data protection requirements¹⁵. The size and weight of laptops/devices mean that they are more vulnerable to loss, theft and exposure to unauthorised access than office based PCs. Any loss of data is a security incident, and depending on the circumstances of the loss and resultant risks, the LSB could incur a fine imposed by the Information Commissioner's Office. In working remotely, therefore, colleagues must:

- Immediately report any actual or potential compromise of IT equipment and/or LSB data to the Director of Finance.
- Never leave a laptop or device unattended and unsecured.
- Lock the screen or shut down the laptop/device when not in use.

When laptops/devices are taken away from the office, the physical security controls that are applied within the office environment are not available. To maintain the confidentiality, integrity and availability of data therefore, colleagues should:

- Never leave the laptop/device in an obviously visible location, even at home. If possible, devices should be stored within the confines of a locked cabinet or

¹⁵ See the separate Data Protection Policy

room.

- Never leave a laptop/device unattended in a car, particularly overnight. When in transit, colleagues should store items in the boot and out of sight.
- Never leave a laptop/device unattended in insecure areas, for example next to areas of public access in meeting rooms, and hotel rooms where others may have access. Colleagues should make use of room locks and lockable storage facilities where available.
- When travelling, avoid placing laptops in locations where they could be easily forgotten or left behind such as in overhead racks and taxi boots.
- Be aware that the use of laptops/devices in public places will draw the attention of those in the area. It is possible that information viewed on a laptop screen/device could lead to unauthorised disclosure of that information.

Where colleagues wish to use their own devices as a work tool, it is their responsibility to maintain the security of any information retrieved from LSB systems.

Colleagues should also note the following:

- Colleagues must never email **personal data** from LSB systems onto their own devices. They should avoid sending information containing personal data via public email systems.
- The LSB may refuse, prevent or withdraw access to colleagues and/or

The following email disclaimer, which covers the key legal requirements, is added automatically to every email sent from our system: *"This e-mail (and any attachment) is intended only for the attention of the addressee(s). Its unauthorised use, disclosure, storage or copying is not permitted. If you are not the intended recipient, please destroy all copies and inform the sender by return e-mail."*

"Internet e-mail is not a secure medium. Any reply to this message could be intercepted and read by someone else. Please bear that in mind when deciding whether to send material in response to this message by e-mail."

"This e-mail (whether you are the sender or the recipient) may be monitored, recorded and retained by the Legal Services Board. E-mail monitoring / blocking software may be used, and e-mail content may be read at any time. You have a responsibility to ensure laws are not broken when composing or forwarding e-mails and their contents."

"The Legal Services Board is a public authority subject to the Freedom of Information Act (FoIA) 2000. The content of this email (and any reply) may be disclosed in response to a request for information, unless it constitutes exempt information under Part 2 of FoIA 2000."

Online purchasing

Colleagues may purchase goods online, whether for personal purposes, or on behalf of the LSB, but must ensure that:

- the vendor is reputable;

- the website is secure;
- any IT security measures, privacy policies or terms of access do not compromise the LSB; and
- payment is made in accordance with the agreement entered into and does not compromise the LSB. Where the purchase in question is on behalf of the LSB, colleagues should make sure they are complying with the LSB procurement rules as set out in the *Finance Manual*.

8. Use of laptops and personal devices

There are LSB laptops available for all colleagues' use, to enable home working (with remote access to standard LSB systems). Colleagues are also permitted to use their own equipment (PC, laptop or Mac) to access LSB systems, subject to the conditions set out in paragraphs 8.4 and 8.5 below, and any supplementary guidance provided. No data can be stored on a remote device when connected to the LSB system as users are effectively 'working on the server' and files never leave the LSB server. (This does not apply to any attachments that may be sent to personal email accounts).

In relation to the use of both LSB issued laptops and own devices for work purposes, colleagues should ensure that they adhere to confidentiality, integrity and data protection requirements¹⁶. The size and weight of laptops/devices mean that they are more vulnerable to loss, theft and exposure to unauthorised access than office based PCs. Any loss of data is a security incident, and depending on the circumstances of the loss and resultant risks, the LSB could incur a fine imposed by the Information Commissioner's Office. In working remotely, therefore, colleagues must:

- Immediately report any actual or potential compromise of IT equipment and/or LSB data to the Head of Finance.
- Never leave a laptop or device unattended and unsecured.
- Lock the screen or shut down the laptop/device when not in use.

When laptops/devices are taken away from the office, the physical security controls that are applied within the office environment are not available. To maintain the confidentiality, integrity and availability of data therefore, colleagues should:

- Never leave the laptop/device in an obviously visible location, even at home. If possible, devices should be stored within the confines of a locked cabinet or room.
- Never leave a laptop/device unattended in a car, particularly overnight. When in transit, colleagues should store items in the boot and out of sight.
- Never leave a laptop/device unattended in insecure areas, for example next to areas of public access in meeting rooms, and hotel rooms where others may

¹⁶ See the separate Data Protection Policy

have access. Colleagues should make use of room locks and lockable storage facilities where available.

- When travelling, avoid placing laptops in locations where they could be easily forgotten or left behind such as in overhead racks and taxi boots.
- Be aware that the use of laptops/devices in public places will draw the attention of those in the area. It is possible that information viewed on a laptop screen/device could lead to unauthorised disclosure of that information.

Where colleagues wish to use their own devices as a work tool, it is their responsibility to maintain the security of any information retrieved from LSB systems.

Colleagues should also note the following:

- Colleagues must never email **personal data** from LSB systems onto their own devices. They should avoid sending information containing personal data via public email systems.
- The LSB may refuse, prevent or withdraw access to colleagues and/or particular devices or software, where it considers that they present unacceptable security or other risks.
- Loss or theft of the device, or suspicion that its security has been compromised must be promptly reported to the Director of Finance.
- The LSB will not monitor the content of personal devices, but it reserves the right to monitor data traffic between such devices and LSB systems.
- Information held on colleagues' own devices is subject to the provisions of the FOIA, if it relates to official LSB business (saved emails)
- The LSB, as data controller, remains in control of all data held on and generated from its systems, regardless of the ownership of the device.

9. Monitoring

The LSB accepts that the internet and email are valuable business tools. However, misuse can have a negative impact on colleagues' productivity and the reputation of the organisation and any third parties. In addition, all of the LSB's internet-related resources are provided for business purposes.

Use of the internet and email will therefore be monitored to ensure that the security of the networks, systems equipment and integrity are not compromised. We reserve the right to survey, record and retrieve all information from our electronic communication systems including (but not limited to) telephone use, emails and internet usage, recording the time of use, the locations visited and the content retrieved. Emails sent and received by colleagues can be recovered by the LSB even after deletion.

We recognise that colleagues have a legitimate right to expect that their personal life remains private. We will therefore take all reasonable steps to ensure that the principles relating to processing of personal data contained in the GDPR are followed when such monitoring is carried out. All information gathered as a result of monitoring will be held securely, with only certain authorised personnel being allowed access to such information.

Reasons for monitoring

Where information has been gathered as a result of monitoring, this will usually only be used for the purpose for which the monitoring was carried out. However, there may be circumstances where monitoring for one purpose (e.g. monitoring inboxes when colleagues are on sickness absence), leads to the discovery of an activity that we could not reasonably be expected to ignore, for example, discovery of a serious breach of health and safety rules that puts others at risk. Clearly, in such circumstances, we reserve the right to take such action as is necessary to protect the LSB's interests, and those of third parties.

We want to provide a working environment free from bullying, harassment and discrimination. In order to detect such unacceptable behaviour, as well as to protect the LSB against liability for the wrongdoings of its colleagues, it may be necessary for the LSB to monitor the use by colleagues of its electronic communication systems to establish whether there is reason to believe that such behaviour has taken place.

9.6 We may also need to carry out monitoring for business purposes in order to ensure that colleagues do not breach other LSB Policies, such as the rules about breaches of confidentiality, which are set out in the LSB Confidentiality Policy.

Monitoring may be required to investigate allegations of misuse or abuse of the electronic communication systems made in the context of disciplinary procedures. For example, monitoring might be necessary as a useful tool to counter time wasting and detect excessive personal use, which can cause an unnecessary burden on colleagues who have to cover for colleagues who spend unreasonable amounts of time emailing friends or browsing the Internet.

We may need to check a colleague's inbox when he or she is absent from work to determine whether there are any emails or voice mails that require attention during such absence. We may also need to monitor communications for colleague training and quality control purposes.

Resource monitoring reports will be made available to the Director of Finance to ensure that resources are used in compliance with this Policy.