Information Security Policy

The sixth data protection principle requires that organisations employ appropriate technological and organisational measures to ensure the security of personal data. In this policy OASEE has set out the processes which must be followed to keep data secure (organisational measures), and the technological measures which must be adopted.

Scope of this policy

This policy applies to everyone who processes personal data from or on behalf of OASEE. This includes Intergroup officers, representatives and OA members. All are responsible for ensuring that if they deal with any personal data, it is kept securely and is not disclosed (either orally or in writing or accidentally) to any unauthorised third party.

General principles

OA is an anonymous fellowship, and our 12th Tradition states that: “Anonymity is the spiritual foundation of all these Traditions, ever reminding us to place principles before personalities”. We hold information about other fellows in confidence. This policy upholds the 12th Tradition.

Personal information must not be shared informally, nor disclosed to people who are not authorised to see it. Data must be kept secure, and if it is no longer required, it must be securely deleted or destroyed. If data is lost or stolen then this must be reported as soon as this is realised, following the procedure in this document. Particular care must be taken when data is transferred from one place to another to ensure that it is not lost in transit.

Hard copy documents

When personal data is stored on paper (for example: a register of meeting attenders), it must be kept in a secure place where unauthorised people cannot see it.

When not required, paper or files must be kept in a locked drawer or filing cabinet.

Printouts must not be left where unauthorised people could see them, like on a printer, or on the kitchen table.

Paper copies must be securely shredded or burned when no longer required. Tearing or screwing up paper is not a secure means of disposal.

Most OA meetings or events use 'We Care' books and lists. These should be destroyed after every meeting, once people have had the opportunity to copy the information they need. Photographing the pages should not be allowed.

Electronic data

Computers and devices used to access personal data must have current software installed, as legacy software is not supported by security patching. Security updates should be installed. Devices should always anti-virus / anti-malware software installed, and kept updated.

Strong passwords must be used to secure electronic devices and also services used to access data (email, dropbox, Microsoft account etc). Passwords must not be reused, shared, saved to file, or saved to non-secure password key chains or browsers. Password management software should ideally be used, and protected with a strong password. Guidance on choosing and using passwords can be found here.

If using a shared computer, password protected services must be closed down when work is finished. Files and folders must not be left open, and the screen must be locked when away from it.

Home Wi-Fi must be encrypted to the highest standard available (ideally WPA2). Suggestions for securing home Wi-Fi are:

- Change your router admin username and password so that they are not the standard for your router.
- Change the broadcast name for your Wi-Fi (the SSID) so that it does not describe the router.
- Activate firewalls and turn off guest networks.
- Keep firmware updated.
- Unless your router is locked away, turn off WPS (the one-push button to connect to your router).

Open Wi-Fi networks must not be used to access personal data.

Mobile devices

Particular care must be taken to keep mobile devices secure: they must be password protected, and ideally encrypted. Unencrypted USB devices are especially insecure as they are so easy to lose. Ideally devices should have remote wiping agents installed so that they can be erased if stolen.

Dropbox

OASEE officers make use of Dropbox (basic) to save information. Two-step verification must be activated, and a strong password used.

Documents must be saved in the correct location as per the template, and multiple copies of the same documents not allowed to proliferate. Any document which contains personal data must be saved using a filename with the suffix PD, for example: 'Website Invoices (PD)'. Each officer is responsible for their own Dropbox folder.

Documents must be deleted in line with the archiving and retention rules set out in the Privacy Policy.

The Website Officer is the Dropbox Administrator. They will manage access to Dropbox folders, ensuring that access is only granted to current Officers, and outgoing Officers conducting a handover. Once an Officer has completed their handover then they will be removed from shared folders, and synced copies of information removed from their personal Dropbox by the Administrator.

Email

Intergroup officers, representatives, and OA members will make use of their personal email accounts for OA business. Officers also have use of the OASEE email system, hosted by Global Gold.

Email is not inherently secure. Most emails transmitted over the internet are sent in plain text, which makes them vulnerable to interception. Consider what information is sent via email.

It is strongly suggested that generic email addresses are used wherever possible, i.e. that officers use their oasouthandeastengland addresses, and that OA meetings make use of generic addresses. At least one generic meeting email address be created for each OA meeting. This would pass from member to member as service positions are rotated. One might be held by the meeting Intergroup rep (for example, igrepbeaconsfieldoa@gmail.com) to which all IG related information and announcements can be sent by the IG Executive Secretary. Another might be held by a member willing to answer questions about their meeting or any event that might be being hosted. For example, infobeaconsfieldoa@gmail.com This will minimise the use of personal email addresses either inside or outside of OA.

Email accounts must be securely password protected, and security features not disabled.

Great care should be taken when opening email attachments, in case they contain a virus, Trojan, spyware or other malware. It is now commonplace for ransomware attacks to be launched by 'spoof' emails which appear to come from a legitimate organisation (for example HMRC) attaching an invoice or order form, which, if opened, installs malware which encrypts all data on the attacked device. A ransom is then charged for the decryption key. Under the GDPR corruption of data is a data breach, and therefore a ransomware attack should be reported as such to the Chair of SEEIG, as per the policy below.

When sending emails to a list, the email must be addressed in the 'To' field back to the sender, with the recipients listed in the 'BCC' (blind carbon copy) field. This means that email addresses are not shared between the whole list.

Documents containing personal data may be attached to emails, either sent or received. These must be saved securely. The emails with the attachments must also be kept secure, and themselves deleted in accordance with the archiving and retention rules set out in the Privacy Policy.

Data breach

Reporting to Chair of OASEE

The GDPR requires that OA notify the Information Commissioners Office of a data breach without undue delay, and not later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of data subjects.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This might include loss of a USB stick with OA members' contact details, or accidental email of contact details to anyone not authorised to receive them.

Anyone handling personal data in connection with OA (Intergroup officers, representatives, and OA members in general) must notify the Chair of SEEIG as soon as they become award of a data breach (chair@oasouthandeastengland.org.uk). Anyone who has concerns about data privacy or the risk of a breach should notify the Chair of their concerns.

Notification to ICO

The Chair will consider whether the breach is likely to result in a risk to the rights and freedoms of data subjects. If such a risk is unlikely then the breach will not be reported to the ICO, but will be recorded in the data breach template. Remedial action will be identified, and a timetable for completion will be drawn up.

If there is a risk to data subjects, the Chair will notify the ICO of the breach, describing:

a) the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
b) the name and contact details of the person from whom more information can be obtained. This may be the Chair, or it may be some other person assigned responsibility for handling the data breach
c) the likely consequences of the personal data breach
d) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

This notification will take place within 72 hours of the Chair being notified of the breach, unless this is not possible, in which case it will take place as soon as possible, and reasons given for the delay.

Where it is not possible to provide all of the above information at the same time, the information may be provided in phases without undue further delay.

The Chair will record the breach in the template, stating the nature of the breach, when and how it was reported, when it was notified to the ICO, its effects and the remedial action taken, and any response from the ICO, including any mandated action.

Notification to data subject(s)

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, and it is not possible to prevent this risk from materialising, the Chair will inform the data subject(s) without undue delay. The following information will be communicated, using clear and plain language:

a) The nature of the personal data breach
b) the name and contact details of the person from whom more information can be obtained. This may be the Chair, or it may be some other person assigned responsibility for handling the data breach
c) the likely consequences of the personal data breach
d) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

The notice must be sent directly to the data subject, unless this would involve disproportionate effort, in which case it can be published on the website.

Delegation

The Chair may delegate their responsibilities under this section to a named person, but will continue to hold ultimate responsibility for ensuring that any breach is properly recorded and (if relevant) notified.

Version

This policy was drafted on 14th April 2018, and approved by the OASEE Intergroup on [INSERT DATE]. It should be reviewed by 31st May 2019.

Any questions about this policy or any queries concerning data protection matters should be raised with the Chair of SEEIG (chair@oasouthandeastengland.org.uk)