OVEREATERS ANONYMOUS®

South and East England Intergroup

POLICIES

21 May 2018

OA South & East England Intergroup, BM Box 6367, London WC1N 3XX
07583 533090| www.oasouthandeastengland.org.uk |

POLICY: THE UPHOLDING OF THE TRADITIONS (JANUARY 2001)

It is this Intergroups (IG) responsibility to support groups in upholding the Traditions. If the IG becomes aware that any of the Traditions appear to be broken by a group, IG undertakes to take the following course of action:

- Two members of IG will visit the meeting as IG Representatives (Reps) in order to clarify and hopefully resolve the issue. The IG Reps will explain the breach in the Traditions and discuss the situation with the group. If the matter can be resolved successfully at this time, the IG Reps will report back to the next IG that the matter is resolved and confirm this in writing to the group.
- Alternatively, if the matter cannot be immediately resolved, the IG Reps will ask the group to take a group conscience and set a date (one month from the date of the visit) for the group to contact the IG Reps with the results of their group conscience. A further visit to the group by IG Reps to help with a clarification may be arranged if requested. If the matter has been resolved the IG Reps will report back to next IG meeting that the matter is resolved and confirm this in writing to the group.
- If resolution has still not been achieved, and the Traditions still appear to be broken by the group, the IG Reps will inform the group that the matter will be discussed at the next IG meeting, where further action will be decided. A representative and/or other member of the group will be encouraged to attend and to participate in the discussion. The group will be informed of the IG's decision in writing. If in IG's opinion, a group has persisted in breaking the traditions of OA, in spite of IG representations, the IG decision may include as a last resort, removal of the group from the list of meetings.

Rationale:

- Tradition 4: Each group is autonomous, except in matters affecting other groups or OA as a whole.
- The series of actions outlined above respect an individual group's autonomy whilst recognising that breaches of the Traditions have an impact on OA as a whole and therefore cannot be ignored.
- The aim is to be supportive as sometimes all that is required that the breach be brought to the notice of the group. It is quite possible for such a breach to occur unintentionally.

The actions proposed will help IG to deal with any breach in a more systematic way and limit the time taken to achieve a resolution of the problem.

POLICY: ELECTION OF OFFICERS TO MULTIPLE POSTS (NOVEMBER 2008)

Following the September 2008 IG election of representatives to stand for election at the National Assembly as NSB Officers, the November 2008 meeting asked that the following policy document be recorded: "In future we should think carefully before electing one officer into three different positions."

POLICY: EMAIL DISTRIBUTION OF MINUTES (SEPTEMBER 2014)

1. All IG Reps will provide an email address to the Executive Secretary.
2. The minutes of IG meetings will be made available electronically to registered IG reps and/or an OA member designated by a group to receive IG communications.
3. If for any reason a member is unable to access minutes or documents electronically. The Intergroup will support them in finding a suitable way to access the minutes/documents, which could be providing a paper copy.

POLICY: EXPENSES (MARCH 2009, EXPANDED JANUARY 2010, AMENDED JULY 2013, AMENDED AND EXPANDED OCTOBER 2016, AMENDED MARCH 2018)

OA South & East England Intergroup (OASEEIG) Officers may incur expenses as a result of performing their elected service roles. The treasurer of OASEEIG is responsible for reimbursing IG Officers for the following types of expenses:

1. Travel costs
2. Stationary costs (including postage costs, stamps, envelopes and financial ledgers used solely for IG work
3. Website software for the operation of the OASEEIG website
4. Actual photocopying/printing expenses or a rate of 7 pence per page for printing at home, for the production of the IG pack and documents for the IG meetings
5. OA literature to support the IG Officers' work such as HIPM and Public Information Guides

Travel costs: Officers expenses for the following will be covered when travelling on OA business:

1. Cost of return second/economy class travel to the location.
2. Cost of a taxi or public transport when necessary as part of the journey.
3. Payment of 35p per mile driven.
4. The hotel charge for a standard room and breakfast for the duration of the event. Officers will be expected to share rooms for overnight stays where possible. The officer has the option to pay a single room supplement.
5. When travelling to the WSBC in New Mexico SEEIG will pay for up to seven nights' accommodation in New Mexico so that the rep may travel in the day before the conference starts and adjust to the time change.
6. Reasonable costs incurred in respect of the OASEEIG telephone helpline.
7. £20 per day food allowance if meals are not included in the hotel/conference arrangements.
8. Delegates travelling overseas are expected to arrange their own travel insurance cover. Reasonable travel insurance and visa costs will be reimbursed by IG where necessary.
9. A float may be given in advance where necessary.
10. Any upgrades to this policy will be paid for personally. It is assumed that all members will be frugal with OA funds at all times.

Costs which cannot be reimbursed by OASEEIG include care costs (e.g. child care, adult care costs etc.) All expenses must be accompanied by a receipt (wherever possible) and an expense form.
Any other expenses which fall outside the scope of the above criteria must be submitted to the IG Board for review and consideration. The board will then decide whether this expense can be reimbursed.

No IG signatory should sign cheques made out to him/herself for reimbursement of IG expenses, but instead should have these signed by another IG signatory, unless agreed by a majority vote of the IG, or in exceptional circumstances by the IG chair

POLICY: PROTECTION OF VULNERABLE NEWCOMERS (JANUARY 2010)

Information to groups about how to protect vulnerable newcomers from predatory sexual behavior in meetings. In previous intergroup meetings the following advice has been given:

1. Have two greeters, one of each sex, if possible.
2. Encourage the greeters to introduce new members to members of the same sex.
3. Emphasise in the meeting format that it is suggested that members find help from members of the same sex.
4. If there is concern in your meeting about this issue call a group conscience to discuss it.
5. Remind experienced group members that we all have a responsibility to watch out for new members.
6. If you require more help please contact intergroup.

POLICY: REQUIREMENTS FOR PROFESSIONAL OUTREACH WORK (JANUARY 2010, AMENDED OCTOBER 2016, AMENDED JANUARY 2018)

To be qualified to do professional outreach work on behalf of the intergroup, it is recommended that members:

a) Have a minimum of six months current continuous abstinence
b) Have worked through steps 1-9 and continue to be working steps 10-12
c) Have a working knowledge of OA's 12 steps and traditions
d) Have physical recovery

A member is understood to have experienced physical recovery if they consider themselves

(i) To be in a healthy weight range
(ii) To have made significant progress in approaching a healthy weight range.

POLICY: EVENT FUNDING DECISIONS (JULY 2010, AMENDED OCTOBER 2016)

Funding decisions for public information / professional outreach events and materials shall be brought before the intergroup and determined by group conscience wherever possible.

If the timeline is such that a decision needs to be made before the next intergroup meeting, then a decision can be made by the Executive Committee as trusted servants on behalf of the intergroup.

In making such a decision the board will have regard for the current financial position of the intergroup, the traditions and concepts of service and the likely views of the meeting on such an issue based on their experience at intergroup.

A decision would require at least a ¾ vote in favour, and if possible, a unanimous decision should be reached in such cases.

POLICY: RECOMMENDED CONTRIBUTIONS FROM GROUPS (SEPTEMBER 2016)

Individual groups may send contributions directly to service bodies.

However, SEEIG will now offer to do this for individual groups as an optional service. Individual groups can send contributions to SEEIG. The SEEIG Treasurer will then send on the funds to each of the service bodies in the recommended ratio on behalf of the individual group or an alternate ratio if the individual group wish to use a different ratio to the guidance given.

Based on recent guidance issued by Region 9, contributions by groups are recommended to be given to service bodies in the following ratio:

Local Intergroup - 42%
National Service Board OAGB - 22%
Region 9 - 11%
World Service Office 25%

POLICY: GROUP REPORTING (SEPTEMBER 2016)

IGRs are invited to complete and submit a Group Report Template to the Executive Secretary on the health of their groups in advance of each IG meeting. These will be amalgamated and form part of the Agenda Pack.

POLICY: ANONYMISATION OF MEETING MINUTES (JANUARY 2018, AMENDED MAY 2018)

1. SEEIG meeting minutes should be anonymised in keeping with Traditions 11 and 12.
2. All SEEIG meeting minutes should contain first names only and these should not be accompanied by second names, personal email addresses or telephone numbers.

POLICY: OFFICER ROTATION OF SERVICE (SEPTEMBER 2014, AMENDED OCTOBER 2016)

Members elected to the Intergroup Executive Committee shall no longer serve as an Intergroup Representative (IR) for a meeting. All other officers may serve dual positions as Intergroup Officer and as IR but are encouraged to vacate the IR position when elected as an officer in order to encourage others to serve.

POLICY: FINANCIAL SUPPORT FOR LOCAL GROUPS (NOVEMBER 2017)

If an individual OA group in the South and East England region incurs a debt and requests South and East England Intergroup (SEEIG) to take on the debt the following approach will be taken:

1. Each request will be reviewed separately on a case by case basis by the Executive Committee.
2. As a guiding principle SEEIG will not cover debts incurred by individual OA groups in the region.
3. However, should there be factors that would cause significant difficulties, i.e. affecting the reputation of OA as a whole, then SEEIG would cover the debt.
4. Decisions will be communicated to the SEEIG board as a whole at the next SEEIG meeting in the calendar.

POLICY: JOB DESCRIPTIONS: EXECUTIVE COMMITTEE AND OFFICERS (JANUARY 2013, AMENDED OCTOBER 2016, AMENDED AND EXPANDED JANUARY 2018, EXPANDED MARCH 2018)

The following responsibilities are a basic outline for each officer position. More complete details are contained in the SEEIG Dropbox documents for officers and updated as individuals perform the specified jobs.

General responsibilities for all Officers

1. Shall provide an officer report for each agenda pack describing actions taken since last Intergroup (IG) meeting.
2. Shall save copies of all documents needed to perform officer role in the IG Dropbox and maintain archives as necessary.
3. Shall perform all other necessary duties as prescribed in IG meetings or as requested by Executive Committee.
4. Officers shall support each other and may request help from other officers or IR's as the need arises in performing duties not within the normal scope of their job description.
5. Shall act in accordance with the Data Policy Protection, and related policies, to ensure that personal information is collected and used fairly, stored securely and not disclosed unlawfully.

1. Chair

1. Shall preside at all regular and special meetings of the IG and IG Executive Committee.
2. Shall be responsible for establishing the agenda for all IG meetings and liaising with the Executive Secretary prior to the agenda pack being sent to Intergroup Reps (IRs).
3. May cast the deciding vote to break a tie.
4. May participate in a ballot vote.
5. May attend all standing committee meetings
6. Shall provide the bank with legally required personal information to be held on record by the bank.

2. Vice Chair

1. Shall serve in the absence of the Chair.
2. Shall chair at least one meeting during each year in office.
3. Shall establish and maintain an IG calendar.
4. Shall provide the bank with legally required personal information to be held on record by the bank.

3. Executive Secretary

1. Shall assemble and distribute the IG Agenda Pack to all IG Officers and Reps prior to each IG meeting. Update and distribute IR Welcome Pack.
2. Shall maintain a record of IG officer and IR attendance.
3. Shall maintain the IG Database and the IG Dropbox.
4. Shall update the IG Bylaws and IG Policy manual.
5. Shall keep records in the IG Dropbox of agendas, officer reports, flyers and other IG documents as required. Electronically backup all essential IG documents.
6. Shall apply to WSO for IG permission to use the OA logo every two years.
7. Shall provide the bank with legally required personal information to be held on record by the bank.

4. Recording Secretary

1. Shall record the minutes of all IG and IG Executive Committee meetings.
2. Shall maintain copies of all minutes in the IG Dropbox: a. Approved Minutes of prior IG meetings b. Draft Minutes of most recent IG meeting c. minutes from IG Executive Committee meetings.
3. Shall create a PDF copy of Approved IG Minutes (with personal information removed) and send to the Web Officer to be posted online.
4. Will send a copy of the Draft Minutes of the most recent IG meeting to the Regional Trustee and to the NSB Chair as a cooperative gesture if they wish to receive them.
6. Shall provide the bank with legally required personal information to be held on record by the bank.

5. Treasurer

1. Shall maintain a chequeing and savings account if necessary, for disbursal of IG funds.
2. Shall submit monthly financial reports at each IG meeting.
3. The Treasurer shall be an account holder and signatory on the IG bank account, along with two other IG officers, one of whom is normally the chair. These signatories will continue to serve in this capacity as long as they remain an IG officer, unless otherwise determined by at 2/3rds vote by the IG.
4. Shall set up and maintain a PO Box and send mail on to other officers and to the National Service Board.
5. Shall send on submitted meeting monies on behalf of the individual groups in the ratio recommended by Region 9 (Local IG 42%, National Service Board OAGB 22%, Region 9 11%, WSO 25%), or in alternative proportions if the individual groups indicate that this is their wish.
6. Shall provide the bank with legally required personal information to be held on record by the bank.

6. Website Officer

1. Shall maintain and update the IG website.
2. Shall set up and maintain IG officer email accounts.

7. Newsletter Officer

1. Shall produce and distribute the IG newsletter.
2. Shall maintain newsletter distribution list.

8. Telephone Officer

1. Shall respond to calls and texts made to the IG mobile phone.
2. Shall maintain a list of volunteers to cover for holidays/illness.

9. World Service Delegate

1. Shall report regularly on information received from WSO/WSBC and attend WSBC where necessary and when this can be financed by the Intergroup.
2. Shall present to the IG for discussion Bylaws and Policy proposals (agenda items) when received prior to WSBC.
3. Shall serve on a WSBC committee and report to IG on pertinent actions of their committee work

10. Region 9 Representative

1. Shall report regularly on information received from R9.
2. Shall attend R9 Assembly where necessary and when this can be financed by the Intergroup.
3. Shall participate in R9 service on behalf of the IG (e.g. serving on R9 committees.)

11. National Assembly Delegates

1. Shall report regularly on information received from OAGB.
2. Shall attend OAGB Assembly where necessary and when this can be financed by the IG.
3. Shall undertake service activities at the national level, supporting the work of the NSB.

12. National Service Board Officers

1. Shall attend National Service Board meetings and report new developments to the IG at least four times a year; at least two such reports should be made in person. Communication for NSB Representatives may be carried out by any NSB Representative.

13. Social Media Officer

1. Shall research OA guidelines and policies relating to social media and the Traditions, particularly as they relate to anonymity
2. Shall investigate opportunities for OA to use social media to carry the OA message, and present these to Intergroup for consideration
3. If requested by Intergroup, shall create accounts and post suitable content, respond to messages/enquiries and monitor the accounts for any activity that is in contradiction of the Traditions or likely to bring OA into disrepute
4. Shall work with other officers to ensure consistency of information across our social media accounts, website and newsletter

14. 12th Step Within Committee Chair

1. Shall preside over all meetings of the 12th Step Within Committee.
2. Shall be responsible for establishing the agenda for each committee meeting.

15. Outreach Committee Chair

1. Shall preside over all meetings of the Outreach Committee.
2. Shall be responsible for establishing the agenda for each committee

POLICY: PRIVACY (MAY 2018)

Overeaters Anonymous South and East England (OASEE) upholds our 12th Tradition of anonymity and is committed to protecting the privacy of everyone who shares their personal information with us.

1. Scope of this policy

OASEE will process personal data of OA members and non-members. Individuals may subscribe to the newsletter, members may attend Intergroup meetings, and may act as Officers for Intergroup. Registers will be kept of meetings, and contact details saved to email accounts. If members arrange events or workshops and produce publicity material, then this will be distributed and published to the website.

OASEE is committed to upholding the privacy of individuals whose personal information is being processed, and this policy describes how this commitment will be met. It applies to Intergroup officers, representatives, and OA members who deal with personal data on behalf of OASEE or in connection with OASEE.

This policy should be read in conjunction with the Data Protection Policy and the Information Security Policy.

2. General principles

OASEE takes full responsibility for the personal information we process. Privacy will be protected, and personal information never disclosed, unless with explicit consent, or where this is to a data processor (like Dropbox, or our website hosts) or where this is required by law. We will only use personal data for the purpose which it was disclosed, and securely delete / destroy it once it is no longer required.

3. Intergroup Officers and Representatives

Officers and Representatives will supply their contact details to OASEE so that they can be contacted in order to fulfil their role within OA. If their contact details change they should notify the Executive Secretary (secretary@oasouthandeastengland.org.uk) so that the records can be updated.

The details of the officers / representatives will be held on record for one year after they have left their role. If they have signed a register of attendance at meetings, then this record will be kept for one year after the meeting. Details will not be shared with third parties, save that email addresses will (in the course of their use) be shared with email providers, and information will be held on Dropbox.

If any officer or representative would like to object to the processing of their data, or request that processing be restricted, they should do so in writing to the Chair of OASEE.

4. Events flyers

OA members sometimes supply their contact details in flyers and promotional material for events and workshops. The flyers supplied to OASEE for this purpose will be published on the website. A record will be kept of what information is provided. Once the event has passed then the flyer will be removed from the website, and a request made for Google to delete the record of the flyer.
The website is hosted by Global Gold, and therefore the contact information in the flyers will be processed by Global Gold on behalf of OASEE. Once the flyer has been deleted from the website then it is no longer in the possession of Global Gold.
If the OA member wishes to have the flyer removed prior to the event, then they should contact the Chair of OASEE who will direct the Website Officer to ensure that the flyer is removed.

5. Data subject rights

Under the GDPR, data subjects (people whose data is being processed), have several rights:

a) The right to know what data has been collected about them, and how such data has been processed
b) The right to make changes to inaccurate data
c) The right to withdraw consent to data processing
d) The right to ask for data to be deleted
e) The right to object to data processing, or for it to be restricted
f) The right to data portability (this only applies to automated processing, which does not happen in the context of OASEE)
g) The right to complain to the Information Commissioners Office

If you would like to exercise any of these rights, then please contact the Chair of OASEE.

6. Right to access information

Individuals have the right to access any personal data that relates to them which OASEE holds, and to be given the following information:

- The reason why the data is held
- The source of the data (if not directly from the individual themselves)
- Whether it has been disclosed to anyone else, and if so, who
- How long it will be stored
- The right to request that the data be updated, or deleted, or processing restricted in any way
- The right to lodge a complaint to the Information Commissioners Office
- Whether any automated decision-making was used to process the data

This is called a 'subject access request'. Any person who wishes to exercise this right should contact the Chair of SEEIG via email (chair@oasouthandeastengland.org.uk). The information should be provided within 30 days, without charge. The Chair will always verify the identity of anyone making a subject access request before handing over any information.

7. Process for subject access requests

Any subject access requests should be forwarded to the Chair of OASEE, who should record them in the SAR template.
The individual making the request should be contacted and their identity confirmed, if necessary by a telephone conversation, or by being asked to supply written evidence of their identity.
The Chair should collaborate with other Officers to identify all information which is held concerning the subject. OA does not collect a great deal of personal data, and so it is likely that the information will be limited to their attendance at meetings, and their subscription to the newsletter, however if the person has been an Officer or Intergroup representative then there may be more information, including emails from them and concerning them.
All material should be reviewed, and an assessment made of whether it can be immediately disclosed, or whether disclosure may adversely affect the rights and freedoms of another individual. Information about a third party should not be disclosed, and this can be edited out of documents.
Nothing should be disclosed that might prejudice a legal investigation, or where disclosure would breach some other legal duty. Specialist advice should be sought if there is any concern about whether disclosure should not be made.
The general rule is that material should be disclosed within 30 days of the request being made, although if it will take longer to prepare the disclosure then the subject should be contacted within 30 days and informed of the delay and likely timescale for disclosure. Disclosure must be made within 90 days of the request.

If no information is held about the data subject, then they should be informed.
If information is held but no disclosure is made then the data subject should be informed that no action will be taken on their request, and that they have the right to complain to the ICO.
A brief description of the disclosure should be recorded in the SAR template, together with the timing of any disclosure, and any non-disclosed material, with reasons given for non-disclosure.

8. Archiving and retention

Personal data should only be stored for the minimum period necessary, consistent with the purpose for which it was processed. Once the retention period has elapsed it is the responsibility of the person controlling the data to delete it. Officers are responsible for managing their own Dropbox folders and email accounts, and Intergroup representatives responsible for their group's email addresses.

Description of data	**Period to keep**
Contact details for Intergroup Officers	1 year after leaving office
Register of Intergroup meeting attendance	1 year after attend meeting
Contact details for Intergroup representatives	Anonymous emails are preferred for meeting representative (e.g. GreenwichSatAM@address.com). Otherwise, personal contact details of the representative are kept until they inform OA that they are no longer the representative, or until this information is received from the OA group, or a new representative
Emails	1 year after email received or sent
Financial records (including emails)	6 years after end of financial year to which they relate
Events agenda packs	6 years after event, to enable follow up and accountability, including financial accountability
Dropbox folder contents	Officer access to Dropbox deleted by Dropbox Admin once handover period finished Contents of folders deleted in accordance with this table

9. Version

This policy was drafted on 15 April-2018 and approved by the OASEE Intergroup on 05-May-2018. 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 South and East England Intergroup (chair@oasouthandeastengland.org.uk)

POLICY: INFORMATION SECURITY (MAY 2018)

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.

10. 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 unauthorized third party.

11. 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 authorized 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 realized, 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.

12. 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 unauthorized 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 unauthorized 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.

13. 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, drobox, 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.

14. 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.

15. 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.

16. 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 minimize 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.

17. Data breach

1. 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, unauthorized 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 authorized 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.

2. 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.

3. 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 materializing, 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.

4. 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.

18. Version

This policy was drafted on 14 April-2018 and approved by the OASEE Intergroup on 05-May-2018. 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)

POLICY: WEBSITE (MAY 2018)

1. All documents to be considered for uploading will be checked for personal data. If personal data is contained, then the website officer will consider:

   a) Why the data is in the document;
   b) Has the person whose data is disclosed given their consent for website publication. How and when was this consent obtained and how can it be revoked;
   c) Has the person seen a copy of the privacy notice surrounding the handling of their data;
   d) Has the document to be uploaded been recorded in the Website Document Publication Register;
   e) Does the document contain only the minimal amount of data required;
   f) Is the data accurate;
   g) When will this data be deleted from the website and an Outdated Page Removal request sent to Google docs;
   h) Are the appropriate technical and organisational security measures in place;
   i) What is the perceived privacy risk to the person concerned.

   The website officer will assess whether the processing of the personal data in the document will be in accordance with the six data protection principles in the GDPR, taking into consideration the answers to these questions.
   If the website officer is satisfied that the processing will be GDPR compliant then the document may be published.

2. All documents uploaded that contain personal data will be added to the Website Document Publication Register. Recorded is the date data was received, a description of it, who/where it is from, has consent for upload been given, when is the data to be deleted by and when was it deleted securely and a removal request sent to Google docs.
   The Register is reviewed on a fortnightly basis to endure that is current, accurate and that deletion dates are adhered to.

3. Data received via the Email Subscribers Plugin will be reviewed fortnightly. If persons have requested subscription but not confirmed this by clicking the link provided, the 'Resend Confirmation' button will be clicked. If no confirmation of subscription is received within one month of first request then the personal data held will be deleted.
   As part of the review process, email addresses that have been added since the last review will be downloaded and added to the Newsletter Subscribers Status list in Dropbox. Once the details on that list are confirmed as having been added to the Constant Contact mailing list by the Newsletter Officer, they will be securely deleted from both the Plugin and Dropbox.
   Maximum holding time in either place will be one month from the date of receipt.

4. If, for any reason, the Web Officer is unable to access WordPress or Dropbox then the Officer with backup access to both these document storage areas will be notified and the necessary reviews and/or document deletions carried out by him/her.

5. Personal data from a public source may be uploaded only if the organisation from which it was obtained is either compliant with GDPR or the US Privacy Shield.

6. Backups of the WordPress database will be carried out monthly and the backup file stored in Dropbox.

7. Requests by individuals to access the personal data processed via the website should be directed to the Chair of SEEIG. The website officer will support the Chair to respond to subject access requests in accordance with the SEEIG policy, and the GDPR.

8. Privacy notices will be supplied to all data subjects whose data is processed via the website, and also more generally via SEEIG. These will be published on the website. The website officer will ensure that the most recent versions are uploaded.

9. Any questions concerning this policy, or data protection in general, should be directed to the Chair of SEEIG (chair@oasouthandeastengland.org.uk)