Privacy Protection Policy

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a Europe-wide law that replaces the Data Protection Act 1998 in the UK. It is part of the wider package of reform to the data protection landscape that includes the Data Protection Bill. The GDPR sets out requirements for how organisations need to handle personal data from 25 May 2018. Following Brexit the GDPR is retained in UK Law as the UK GDPR that sits alongside the Data Protection Act 2018.

The GDPR applies to 'personal data/information', which means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. The focus of the GDPR is upon ensuring fairness, transparency, accuracy, security, minimisation and respect for the rights of the individual whose personal data/information we want to process.

Key Details

Approved by Executive committee on:	17 July 2020
Policy became operational on:	17 July 2020
Policy last revised by:	Tim Rolfe, Data Protection Officer
Last revised date:	December 2025
Next review date:	Annually at year start of February

Note: SoBRA does not have to register with the Information Commissioners Office (ICO) as we are a charity. A specific exemption applies to bodies or associations that are not established or conducted for profit. However, the exemption applies only if:

- SoBRA is only processing data for the purposes of establishing or maintaining membership or support for a body or association not established or conducted for profit, or providing or administering activities for individuals who are members of the body or association or have regular contact with it;
- SoBRA only holds information about individuals whose data it needs to process for this exemption purpose; and
- The personal data SoBRA processes is restricted to personal information that is necessary for this exemption purpose.

Introduction

At SoBRA, we are committed to protecting and respecting your privacy.

This Policy explains when and why we collect personal information about people who: are, or apply to be members; support membership and accreditation applications; and who visit our website. This policy sets out how we use the information, the conditions under which we may disclose it to others and how we keep it secure. We may change this Policy from time to time so please check the website occasionally to ensure that you are aware of any changes.

By using our website, visitors are agreeing to be bound by this Policy. Any questions regarding this Policy and our privacy practices should be sent by email to info@sobra.org.uk.

Who are we?

The Society of Brownfield Risk Assessment (SoBRA) has been established to support the growing number of professionals working in land contamination risk assessment. It is a learned society for individuals, with membership drawn from the private, public, voluntary and academic sectors. Its goals are to improve technical knowledge in risk-based decision-making related to land contamination applications and to enhance the professional status and profile of practitioners. SoBRA is a charity.

Responsibilities

Everyone who works for, or volunteers with, SoBRA has shared responsibility for ensuring personal data is collected, stored and handled appropriately.

Each member that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, the following people have key areas of responsibility:

- The Executive Committee is ultimately responsible for ensuring that SoBRA meets its legal obligations.

- The Data Protection Officer is responsible for:
  - Keeping the Executive Committee updated about its data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - Arranging data protection induction advice for new Executive Committee members and members -of sub-groups.
  - Handling data protection questions from the Executive Committee and members.
  - Dealing with requests from individuals to see the data that SoBRA holds about them (also called 'subject access requests').
  - Checking and approving any contracts or agreements with third parties that may handle members' information (e.g. our secure web provider).

- The Website Co-Ordinator/ IT Manager is responsible for:
  - Ensuring all systems, services and equipment used for storing personal data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Ensuring removal of expired member personal data from the website and all systems used for storing data annually in January.

- The SoBRA Accreditation Lead is responsible for:
    - Ensuring removal of all accreditation documentation from the system when a member confirms that they no longer wish to maintain their accredited status.
    - Ensuring that Scrutineers are issued a copy of the current SoBRA GDPR Policy for Scrutineers, and ensuring that Scrutineers confirm that they have deleted personal information on Applicants once an application is completed.
    - Ensuring removal of all documents relating to accreditation applications for currently accredited members, two years from the date of application, except for post-interview DOC7s, professional reports, outcome letters, certificates and CPD checks.
    - Removal of accreditation application documentation from the system for those members that failed to achieve accredited status, two years after the date of application.

How do we collect personal information from you?

We obtain personal information about you when you register as a member of the Society through our membership payment platform, send an email to our inboxes (info@sobra.org.uk, accreditation@sobra.org.uk, CPD@sobra.org.uk and sobra@claire.co.uk), or sign up to attend one of our events (e.g. webinars or conferences). Furthermore, we receive personal information through the accreditation application process. We collect information in the following ways:

- Email
- Online forms and creation of accounts
- Paper forms
- Excel and Word documents
- PDF documents (scans)

What type of information is collected from you?

SoBRA will never collect any unnecessary personal data from you and will not process your information in any way, other than as specified in this Policy (minimisation). We will only use people's data in ways they would reasonably expect and which have a minimal impact on privacy. The personal data that we collect includes:

- Name
- Date of Birth
- Home Address
- Business/ Institute Address
- Personal Email
- Business Email
- Mobile Telephone Number
- Optional alternate Telephone Number (home or work)
- Paypal, Bank or card details (to process payments for membership, conference/workshop attendance, for example)
- Signature (such as on accreditation application forms)
- Status/ Qualifications/ Academic history and CV for those applying for accreditation

Note our members have a personal responsibility to ensure that their personal data is accurate and up to date. This information can be accessed via their personal logins to the SoBRA webpage. Members are responsible also for protecting and not sharing their own login details with others.

How is your information used?

The purposes and reasons for SoBRA using your personal data are:

- processing a payment that you have made;
- processing requests that you have submitted;
- communications relating to outstanding fees;
- carrying out our obligations arising from any contracts entered into by you and us; when seeking your views or comments on the services we provide;
- notifying you of changes to our initiatives;
- sending you communications which you have requested or that may be of interest to you. These may include information about webinars, conferences, partnerships, news, or other initiatives;
- processing a membership, accreditation and /or sub-group application; and
- carrying out three-yearly CPD checks for continuing accreditation.

These uses are necessary for membership contracts and for members' legitimate interests. As a Society, the legal basis of our contractual relationship with our paying membership is the provision of information relating to our core objectives including the dissemination of knowledge regarding land contamination risk assessment (https://sobra.org.uk/about-us/). We will only ever send you communications which you have requested or that may be of interest to you i.e. within the legitimate terms of our core objectives and your membership.

Note: We will review our retention periods for personal information on a regular basis, at least every three years. We are legally required to hold some types of information to fulfil our statutory obligations. We will hold your personal information on our systems only for as long as is necessary for the relevant activity, or as long as is set out in any relevant contract you hold with us.

Who has access to your information?

Only SoBRA approved committee members and selected representatives on a needs-only basis have access to your information. We will not sell or rent your information to third parties. We will not share your information with third parties for marketing purposes. Scrutineers of the accreditation applications process access specific applicants' data, but have access only by a secure shared server with access restricted to those that need the information. In the event that the secure shared server cannot be accessed by an individual, password-protected files will be sent by email and are also bound by the terms and contents of this policy.

Third Party Service Providers working on our behalf

We may pass your information to our third-party service providers for the purposes of completing tasks and providing services to you on our behalf (for example to process payments, send you mailings or process accreditation applications). However, when we use third-party service providers, we disclose only the personal information that is necessary to deliver the service and we have a contract in place that requires them to keep your information secure and not to use it for their own direct marketing purposes.

Please be reassured that we will not release your information to third-parties beyond SoBRA, unless you have requested us to do so, or we are required to do so by law, for example, by a court order or for the purposes of prevention of fraud or other crime.

Third Party Product Providers we work in association with

When you are using our secure online payment pages, your payment is processed by a third-party payment processor, who specialises in the secure online capture and processing of credit/ debit card transactions. If you have any questions regarding secure transactions, please contact us. We do not have access to or save your credit/debit card details.

We may transfer your personal information if we are under a duty to disclose or share your personal data in order to comply with any legal obligation or to enforce or apply our terms of use or to protect the rights, property or safety of our members. However, we will take steps with the aim of ensuring that your privacy rights continue to be protected.

Your choices (consent)

You have a choice about whether or not you wish to receive information from us. If you do not want to receive email communications from us about the work we do and our webinars, conferences or other services, then you can unsubscribe at any time.

Consent is not a precondition of service. Furthermore our obligations do not end when we first get consent. SoBRA will continue to review consent as part of our ongoing relationship with members and refresh it if anything relevant changes.

How you can access and update your information

The accuracy of your information is important to us. You can check and change your information at any time by checking your account details when logging into your SoBRA account, or by emailing info@sobra.org.uk (right to rectification and data quality).

All individuals who are the subject of personal information held by SoBRA are entitled to:

- Ask what information SoBRA holds about them and why.
- Ask how to gain access to it.
- Be informed on how to keep it up to date.
- Be informed on how SoBRA is meeting its data protection obligations.

If an individual contacts SoBRA requesting this information, this is called a 'subject access request'. Subject access requests from individuals should be made by email, addressed to the Data Protection Officer, at info@sobra.org.uk. Individuals will be charged £10 per subject access request. SoBRA must provide information without delay and at least within one calendar month of receiving it. SoBRA can extend this by a further two months for complex or numerous requests (in which case we must inform the individual and give an explanation). Before handing over any information, the Data Protection Officer will always seek to verify using "reasonable means" the identity of anyone making a subject access request.

Right to erasure including retention and disposal

Individuals have the right to be forgotten and can request the erasure of personal data when:

- it is no longer necessary for the purpose SoBRA originally collected/ processed it for;
- the individual withdraws consent;
- SoBRA is relying on legitimate interests as its basis for processing, but the individual objects to the processing of their data, and there is no overriding legitimate interest for SoBRA to continue this processing; or
- it was unlawfully processed (i.e. otherwise in breach of the GDPR).

Individuals can make a request in writing. SoBRA will seek to verify the identity of the person making the request, using "reasonable means". SoBRA should respond to a request without delay and at least within one month of receipt.

A written retention policy (see **Appendix A**) will be used to remind SoBRA when to dispose of various categories of data, and help SoBRA plan for its secure disposal. SoBRA will designate responsibility for retention and disposal to an appropriate person.

We employ the following security precautions to prevent the loss, misuse or alteration of any personal information held by our organisation:

- All our information on members is held in secure servers with up to date firewalls, encryptions and strong password protection.
- All members are required to use a strong password to protect their individual account.
- The back end of the website has restricted access to the website designer, Secretary and the Website Co-Ordinator.
- PayPal handles all our members' bank details and these details are not kept anywhere else.
- PayPal has extensive security measures in place and the only persons that will access Paypal are the SoBRA Treasurer, Website Co-Ordinator and the website designer.
- Any personal information held in the Executive Committee Google Drive is only accessible to the current Executive Committee Members. Google security includes two stage verification, strong passwords and 256-bit Advanced Encryption Standard.
- Personal information relating to applicants to the Accreditation scheme and currently accredited members is stored on a secure shared server which is managed by CL:AIRE. Information on this secure shared server is available to the SoBRA Accreditation Lead, the CPD Co-Ordinator, and the Website and Membership Co-Ordinator only, and access to the folders is restricted as required. During an application window, Scrutineers may temporarily store local copies of an Applicant's personal information as encrypted documents. After the accreditation process has been completed for an individual, the Scrutineers must confirm in writing to the Accreditation Scheme Administrator that they have permanently deleted any local copies from their drives and email accounts.

Data/information relating to sub-groups may be stored on separate Dropbox or Google Drive accounts and will be transferred to the Executive Committee Google Drive by sub-group Leads or the sub-group Executive Committee sponsor on an annual basis each April. This will not normally include 'personal data/information', although attendee lists for conferences would meet the definition. These sub-group Dropbox accounts will be accessible to the relevant sub-group members and current Executive Committee Members only.

Profiling

We do not analyse, or plan to analyse, your personal information to create a profile of your interests and preferences.

Use of 'cookies'

The SoBRA website does not use cookies, other than Google Analytics, and session cookies from WordPress & WPEngine.

Links to other websites

Our website may contain links to other websites run by other organisations. This policy applies only to our website, so we encourage you to read the policy statements on the other websites you visit. We cannot be responsible for the policies and practices of other sites even if you access them using links from our website.

In addition, if you linked to our website from a third-party site, we cannot be responsible for the policies and practices of the owners and operators of that third-party site and recommend that you check the policy of that third-party site.

The processing of children's personal data

SoBRA membership does not include ages 16 or under and its processing or ownership of children's personal data is not considered applicable.

Transferring your information outside of Europe

As part of the services offered to you as a SoBRA member or through our website, the information which you provide to us may be transferred to countries outside the European Union ("EU"). By way of example, this may happen if any of our servers are from time to time located in a country outside of the EU. These countries may not have similar data protection laws to the UK. By submitting your personal data, you are agreeing to this transfer, storing or processing. If we knowingly transfer your information outside of the EU in this way, we will take steps to ensure that appropriate security measures are taken with the aim of ensuring that your privacy rights continue to be protected as outlined in this Policy.

Website recording

The SoBRA website does not undertake website recording of any kind. Webinars provided by SoBRA or third-parties may be recorded by the host provider and the recordings made available to members through a third party website. Please refer to the "Links to other websites" Section above.

Review of this Policy

SoBRA commits to keep this Policy under regular review. This Policy was last updated in November 2025. It is intended that it will be reviewed as a minimum annually.

Data Breach

The GDPR introduces a duty on all organisations to report certain types of personal data breaches to the Information Commissioner's Office (ICO) and, in some cases, to the individuals affected. 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.

We have to notify the ICO of a breach unless it is unlikely to result in a risk to the rights and freedoms of individuals. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we must notify those concerned directly and without undue delay. Information on the definition of a data breach and when a breach is notifiable is provided on the ICO website at: https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/personal-data-breaches.

In all cases we must maintain records of personal data breaches, whether or not they are notifiable to the ICO.

We would report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. The GDPR recognises that it will not always be possible to investigate a breach fully within that time-period and allows us to provide additional information in phases, so long as this is done without undue further delay.

Our internal breach reporting procedure will be reviewed annually. In light of the tight timescales for reporting a breach it is important that we have robust breach detection, investigation and internal reporting procedures in place.

General Guidelines for SoBRA Members

- The only people able to access personal data covered by this policy should be those who need it for their work and delivering the interests of the individual and SoBRA.
- Data will not be shared informally.
- SoBRA will provide this guidance to its current Executive Committee, new committee members, accreditation scrutineers and website designer to help them understand their responsibilities when handling data.
- SoBRA representatives should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within SoBRA or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Data storage and use

These rules describe how and where personal data should be safely stored. Questions about storing data safely can be directed to the SoBRA Data Protection Officer.

When personal data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to personal data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Paper and printouts should not to be left where unauthorised people could see them, such as on a printer.
- Personal data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Personal data should be protected by strong passwords that are changed regularly and never shared.
- If data is stored on removable media (e.g. CD, DVD or USB drive), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested annually.
- Personal data should never be saved directly to laptops or other mobile devices like tablets or smart phones (with exception of temporary storage of accreditation applicants' encrypted information by scrutineers, as described above).
- All servers and computers containing data should be protected by approved security software and a firewall. The Data Protection Officer is to annually document and update a listing of IT security measures as part of the GDPR audit.
- Personal data should not be shared informally. In particular, it should never be sent by email unless the relevant files have been encrypted and password-protected, as email communication is not secure.
- Data must be encrypted before being transferred electronically.
- SoBRA representatives should not save copies of personal data to their own computers, with the exception of scrutineers who may temporarily hold password-protected encrypted copies of applicant's application forms on computers, or cloud storage operated by an approved operator such as Microsoft, Google, Dropbox, Apple or Amazon. At the end of the application window all scrutineers will be required to confirm in writing that they have permanently deleted copies of applicant's personal information from their local drives, cloud storage and email.
- Always access and update the central copy of any personal data.

Appendix A

Data Retention Policy

- Expired member personal data will be removed from the website and all systems used for storing data annually in January.
- All SoBRA Accreditation application information is retained for two years, whether accreditation is awarded or not.
- After two years, all personal data, except for post-interview 'Assessment Report Forms' (DOC7s), professional reports, outcome letters, certificates and CPD checks will be removed from all systems.
- Personal data will be removed from all systems and the website within one month of an accredited member confirming that they no longer wish to maintain their accreditation status.

Other GDPR Milestones

- The Data Protection Officer is to be named annually and recorded in the Executive Committee meeting minutes.
- The Website Co-Ordinator/ IT Manager is to be named annually and recorded in the Executive Committee meeting minutes.
- The Data Protection Officer will complete a GDPR audit against this policy annually in February, and save a record of the findings in the GDPR folder on the SoBRA Google Drive.
- The internal breach reporting procedure will be reviewed annually in January.
- Data backups should be tested annually in January.
- All servers and computers containing data should be protected by approved security software and a firewall. The Data Protection Officer is to annually document and update a listing of IT security measures as part of the GDPR audit.
- Subject access request responses to be issued within one month, or a further two months for complex or numerous requests.