



Privacy Policy

1. About this policy

InSiGHT is a Charity incorporated in England, governed by its Council according to its Articles of Association. InSiGHT Council and its membership are subject to the laws governing privacy in the United Kingdom. This privacy policy details how InSiGHT handles personal information.

This policy pertains to the Society; the activities of the InSiGHT genetic variant databases and Variant Interpretation Committees (VIC) are covered by an additional policy, and overseen by the VIC Governance Committee.

2. Overview

This privacy policy sets out how InSiGHT uses and protects any information that it is given. InSiGHT needs to gather and use certain information about individuals. InSiGHT is committed to ensuring that privacy is protected. This policy describes how this personal data is collected, handled and stored to meet the organisation's data protection standards in compliance with GDPR legislation. InSiGHT collects, holds, uses and discloses personal information to carry out the functions and activities of coordinating the Charity. These functions and activities include:

- maintaining the register of members of InSiGHT
- facilitating the organisation and running of events and conferences
- producing and distributing information about InSiGHT and its activities
- curating and determining pathogenicity of variants relating to genes determining risk for gastrointestinal hereditary tumours
- other activities as set out under Section 5 (Powers) of its Articles of Association

3. Collection of personal information

We require your consent for all personal data to be collected through our website. All forms require an 'opt in' field to be checked to ensure that you are happy for us to collect your data. By selecting this option and submitting a form, you are agreeing to the policies outlined on this page. At all times, InSiGHT endeavours to only collect the information needed for the particular function or activity being carried out.

The main way personal information is collected is when members or others provide it. For example when people:

- contact the secretariat to ask for information, in order for the

- InSiGHT secretariat to reply
- apply to become a member of InSiGHT, so that InSiGHT secretariat can answer membership queries and approve membership applications
- register for an event that InSiGHT is running or involved in, to enable InSiGHT to notify them of relevant information
- join InSiGHT, to ensure that member lists are up to date and information is only sent to current members
- join Council or a working group, to enable communication to allow the business of the group to be undertaken
- participate in a meeting or consultation with InSiGHT, to enable communication

4. Our website

InSiGHT maintains the International Society for Gastrointestinal Hereditary Tumours website (<https://www.insight-group.org>). The information collected about individuals via this website is stored on secure servers managed according to this policy.

4.1 Website analytics

A range of tools provided by third parties (for example: Google) to collect or view website traffic information is used. These providers have their own privacy policies.

4.2 Cookies

The website uses cookies, as almost all websites do, to help provide the best user experience possible. Cookies are small text files that are placed on the computer or mobile phone when browsing websites.

Cookies:

- make the website work as expected
- avoid having to login every time a user visits the site
- improve the speed/security of the site
- allow sharing of pages with social networks like Facebook
- personalise the site to help users get what they need faster
- continuously improve the website
- make services more efficient

InSiGHT does not use cookies to:

- collect any personally identifiable information (without express permission)
- collect any sensitive information
- pass data to advertising networks
- pass personally identifiable data to third parties
- pay sales commissions



The information collected by cookies may include the IP address of the device of the user and information about sites that IP address has come from, the pages accessed on the InSiGHT site and the next site visited.

If the settings on the software that an individual is using to view the InSiGHT website are adjusted to accept cookies we take this, and the continued use of the website, to mean that the user accepts cookies. Should they wish to remove or not use cookies from our site they can, however doing so will likely mean that our site will not work as expected.

5. Social Networking Services

We may use social networking services such as Twitter, Facebook and YouTube to communicate with the public about InSiGHT. When individuals communicate with us using these services we may collect their personal information, but we only use it to help us to communicate with them and the public. The social networking service will also handle personal information for its own purposes. These sites have their own privacy policies.

6. Email lists

We collect email addresses and, if provided, other contact details when members register and subscribe to our email lists. We only use this information for the purpose of sending regular updates on the activities of the InSiGHT, and to administer the lists.

7. Storage and security of access

We regularly assess the way that we collect, use, store and disclose personal information to ensure its security. Information is stored on secure servers. These are password protected and can only be accessed by the InSiGHT secretariat. Information is deleted when a member does not resubscribe within 30 days of expiry of their membership. Website 'contact us' submission information is stored on the website for 30 days and then will be permanently removed, automatically. We destroy personal information in a secure manner when we no longer need it.

8. Disclosure

We very rarely disclose personal information. When we do, we do so very carefully.

Any email address data collected is never passed on to any third parties, but is made available to other members via the website, with each member's agreement. If a member does not wish other members to have access to their name, institution, country and e-mail address, they can opt out of the 'include in members listing' option when submitting their membership application form, or login and edit their profile later. Members who opt out in this way do not have access to the membership list.



9. Quality of personal information

To ensure that the quality of the personal information we collect we record information in a consistent format, regularly audit our contact lists to check their quality and provide members with a means of updating their own personal information via the InSiGHT website.

10. Access, correction and erasure

Members can access and correct the personal information we have about them by visiting their member profile on the InSiGHT website.

You can also request to access your data and you can request that your data is corrected or removed. You can make this request by email (admin@insight-group.org) in writing (InSiGHT, The Polyposis Registry, St Mark's Hospital, Watford Road, Harrow HA1 3UJ, UK) or by telephone (+44 208 235 4270) to the InSiGHT Secretariat. Any such requests will be completed within 30 days.

11. Data breach

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

While we do everything in our power to prevent this, if a data breach was to occur, we would endeavour to inform the supervisory authority (ICO) within 72 hours. We would also endeavour to inform all affected users about any potential risks which may come as a result of the breach.

If a data breach was to occur, we would document all relevant information and be completely transparent with any users who may be affected. All breaches shall be recorded, including facts relating to the breach, its effects and the remedial action taken. Following a breach, we will ensure that we investigate whether the breach occurred as a result of human error or a systemic issue.

This policy may be amended at the discretion of Council.

Date of Council approval 1st July 2018

Date for review 1st June 2020

