UK Data Protection & Privacy Policy

1.Important Information

Haemochromatosis UK respects your privacy and is committed to protecting your personal data. In this privacy policy, we provide you with information on how we collect, store and use your personal information and tell you about your privacy rights and how the law protects you.

When we refer to personal information, we mean information which identifies you or which could be used to identify you (such as your name and contact details).

It is important that you read this privacy policy, together with any other fair processing notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are fully aware of how and why we are using your information. Haemochromatosis UK has appointed a Data Protection Lead, reporting to the Board of Trustees, who is responsible for overseeing this policy, managing access permissions, and ensuring compliance with data protection law. You can contact them with any questions on how you may exercise your privacy rights at privacy@huk.org.uk.

2.Who we are

We are Haemochromatosis UK (HUK), a charity registered in England and Wales with charity no. 1001307 and SCO41701. We are a Company Limited by Guarantee No. 2541361. We are a controller and we are responsible for your personal information.

HUK's Board of Trustees is ultimately responsible for ensuring the lawful and secure processing of personal information. We operate under a strict data protection governance framework that includes regular audits, data protection training and system access reviews.

3.Access Control and Data Security Governance

We maintain strict access controls over all systems containing personal data. Access is granted only to authorised employees, volunteers and contractors on a role-based and time-limited basis.

- All access permissions are approved by a senior officer or the trustee with data protection oversight
- Access rights are reviewed quarterly or when an individual changes role, and are immediately revoked when an individual leaves HUK
- All access to membership and health-related data is logged and monitored to detect unauthorised activity

- System administrators are required to use multi-factor authentication and strong passwords on all data systems

Any unauthorised access, attempted access, or data breach will be investigated and reported in accordance with our Data Breach Response Procedure (see below).

4.Data Breach Response Procedure

HUK maintains a formal Data Breach Response Procedure. In the event of suspected or confirmed unauthorised access, disclosure, or loss of personal data;

- The Data Protection Lead, or designated trustee will be notified immediately
- Access to relevant systems will be suspended pending investigation
- A preliminary investigation will be completed within 72 hours
- Where required, the Information Commissioner's Office (ICO) and affected individuals will be notified in accordance with Articles 33 and 34 of the UK GDPR

We maintain an internal incident register recording all actual and suspected breaches and remedial actions taken.

5.What data we collect about you

We may collect, use, store and transfer the following kinds of personal information about you:

- **Identity and Contact Data** includes your name, address, email address, telephone number, date of birth, gender
- **Donation Data** includes details of your donations, including your eligibility for Gift Aid
- **Merchandise Shop Data** includes details of shop purchases and delivery information
- **Membership Data** includes details of your membership with HUK, such as membership number, method of payment for membership
- **Technical and Usage Data** includes internet protocol (IP) address, browser type and version, time zone setting and location, browser plug-in types and versions, operating systems and platform, other technology on the devices you use to access our website and information about how you use our website, products and services
  Other 'optional' personal information you may choose to share with us, including through your voluntary use of our online forms or surveys.

We may also collect details of your summary medical data if you choose to share that information with us, so we can better tailor our services to your needs, such as:

- Whether you are a person with genetic haemochromatosis
- A parent or partner of a person with genetic haemochromatosis
- The year of your diagnosis (if applicable)
- How long it took for you to receive a diagnosis (if applicable)

- Your genetic testing status (if applicable)
- Contact details for your clinician of record and/or hospital (if applicable, to enable us to share awareness materials with them anonymously)

We may collect this personal information in a variety of ways, including through our membership application form, through your voluntary use of our online forum or website, if you make a donation to HUK or make a purchase from our shop, or through any feedback, query or other communication you may send us.

6.If you do not provide personal data

Providing your personal information to HUK is voluntary. However, some of the personal information that we request from you is necessary to create your membership to HUK, to provide you with access to our services, to process your donations or to manage any purchases from our shop. If you choose not to provide this information, we may not be able to carry out such actions for you.

7.Why we collect your personal data and how we use it

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal obligation.

Generally, we do not rely on consent as a legal basis for processing your personal information although we will get your consent before collecting any sensitive personal information, such as health-related data, and before sending direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing or our newsletters at any time by contacting us using the 'unsubscribe' link in any of our newsletters.

8.Purposes for using your personal information

We have set out below a description of all the ways we plan to use your personal information, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Purpose / Activity	**Type of data**	**Lawful basis for processing including basis of legitimate interest**
To register you and process your membership	Identity and Contact Data	Performance of a contract with you
To administer Gift Aid claims, ensure that your donations are properly processed and to send you our thanks	Identity and Contact Data Donation Data	Performance of a contract with you
To process any purchases from our shop	Identity and Contact Data Shop Data	Performance of a contract with you
To provide you with access to our online forum and other online benefits, such as access to our website and related materials	Identity and Contact Data Profile Data Technical and Usage Data	Performance of a contract with you
To send you our HUK newsletters if you subscribe to receive these	Identity and Contact Data	Necessary for our legitimate interests (to send you newsletters if you subscribe to receive these)
To administer and protect our charity and website (including troubleshooting data analysis, testing, system maintenance, support, reporting and hosting of data)	Identity and Contact Data Technical and Usage Data	Necessary for our legitimate interests (for running our charity, provision of administration and IT services network security, to prevent fraud and in the context of a business organisation or group restructuring exercise)

		Necessary to comply with a legal obligation
To tailor our services to you and to ensure we provide guidance appropriate to your specific medical needs	Summary medical data	Necessary for your vital interests (for example, when providing guidance in managing your genetic condition) and our legitimate interests in analysing anonymised data relating to the prevalence of genetic haemochromatosis

In all other cases, we will have a legitimate interest, and, in some cases, a legal obligation in processing your personal information before, during and after our relationship with you, in order to allow us to:

- Maintain accurate and up-to-date records and contact details for tax purposes
- Monitor and consider our performance in relation to our charitable objectives
- Conduct medical research into genetic haemochromatosis, from anonymised data in aggregate.

9.Who Has Access to Your Personal Information

We may share your information with the following parties:

- Internally, with employees or volunteers of HUK where necessary to process your information and in accordance with this privacy policy
- Externally, with third party suppliers who provide us with IT, system administration and data storage services as well as other suppliers who provide us with marketing, payment processing, Gift Aid and donations processing, book keeping accounting services, newsletter printing and postage and shop packaging and postage services.

We require all such third parties to respect the security of your personal information and to treat it in accordance with the law. We do not allow our suppliers to use your personal information for their own purposes and only permit them to process it for specified purposes and in accordance with our instructions.

10.Security of your personal information

We take the security of your personal information seriously, and we have put in place appropriate security measures, internal policies and controls to prevent your information from being accidentally lost, used or access in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, volunteers and other third parties who have a business need-to-know. They will only process your personal

information on our instructions and are subject to a duty of confidentiality. We have put in place procedures to deal with any suspected data breach and will notify you and any applicable supervisory authority of a breach where we are legally required to do so.

Some of our suppliers are based outside the UK and European Economic Area (EEA) so their processing of your personal information may involve an international transfer. Whenever we transfer your personal information out of the UK or EEA, we ensure a similar degree of protection is afforded to it by ensuring that adequate safeguards are implemented such as requiring our suppliers to enter in specific contracts approved by the UK government which give personal data the same protection it has in the UK and EEA. Where we use providers based in the USA we may transfer information to them under the International Data Transfer Agreement (IDTA) which requires them to provide similar protection to personal information shared between Europe and the UK.

We implement layered technical and organisational security measures, including encryptions, firewalls, secure backups and regular penetration testing. Access to membership and donation data is restricted to authorised personnel using role-based permissions. All user access and system activity are logges and retained for a minimum of 12 months for audit purposes.

Staff and volunteers with system access are required to sign confidentiality and data protection agreements, and undergo annual data protection training.

11.For how long do we keep your personal information

We will only retain your personal information for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal information for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect of your relationship with you.

To determine the appropriate retention period for personal information, we consider the amount, nature and sensitivity of the information, the potential risk of harm from unauthorised use of disclosure of your information, the purposes for which we process your information and whether we can achieve those purposed through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

12.Changes to this privacy policy and your duty to inform us of changes

We keep our privacy policy under regular review. It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your relationship with us by emailing privacy@huk.org.uk.

13.Your legal rights

When staff, contractors, or volunteers leave the charity their system access is revoked immediately and all associated accounts are securely closed. Backup and archived data are encrypted and accessible only to authorised technical administrators.

Under certain circumstances, you have rights under data protection laws in relation to your personal information. You may be able to:

- Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and the check that we are lawfully processing it
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected, though we may need to verify the accuracy of the new information you provide to us.
- Request erasure of your personal information. This enables you to ask us to delete or remove information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your information where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your information to comply with the law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal information for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms
- Request restriction of processing of your personal information. This enables you to ask us to suspend the processing of your information in certain circumstances
- Request the transfer of your personal information to a third party. We will provide to you, or a third party you have chosen, your information in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- Withdraw consent at any time where we are relying on consent to process your personal information. However, this will not affect the lawfulness of any processing carried out before you withdrew your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

If you would like to exercise any of these rights, please contact us at privacy@huk.org.uk

We may need to request specific information from you to help us to confirm your identity and ensure your right to access your personal information (or to exercise any of your other rights). This is a security measure to ensure that the personal information is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

If you believe that we have not complied with your data protection rights, you have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO, so please contact us in the first instance.

Any individual found to have accessed, retained, or disclosed membership or donor data without authorisation will be subject to disciplinary and/or legal action, including reporting to the ICO and relevant authorities.

14.Contact us

If you have any questions about this privacy policy or our privacy practices, including any requests to exercise your rights, please contact us at privacy@huk.org.uk

The Data Protection Lead (DPL) for the trustees as of 13.11.25 is Pippa Randolph.

Reviewed by the Trustees in November 2025

For further review in November 2027 or earlier if required.