Operating name of the British Allergy Foundation

Client/stakeholder Privacy Policy

Document Number:	Policy Owner:	Board Approval Date:	Date of next review:
AUK.OPS.DOC.03.01	Chief Executive	May 2020	31st May 2026

1. Introduction

1.1 The British Allergy Foundation (Known as Allergy UK), is committed to protecting the privacy and personal data of all individuals whose information we collect and process. As a national charity supporting people affected by allergies, we hold personal and, in some cases, sensitive information in order to deliver our services, meet our legal obligations and operate effectively.

1.2 This policy explains how Allergy UK collects, uses, stores, shares and protects personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable legislation. It also sets out the rights of individuals and our responsibilities as a data controller.

1.3 Allergy UK is registered with the Information Commissioner's Office (ICO) as a Data Controller (registration number Z5226293). We are committed to handling personal data lawfully, fairly and transparently, and to maintaining the trust placed in us by those we support, work with and employ.

2. Scope

2.1 This policy applies to all personal data processed by Allergy UK, regardless of format, including electronic systems, manual records and verbal communications. It covers personal data relating to, but not limited to:

- people living with allergy
- parents, carers and family members
- event attendees
- health professionals
- donors, fundraisers and corporate partners
- manufacturers and suppliers
- journalists and media representatives
- volunteers
- employees and job applicants
- any other stakeholders whose personal data Allergy UK processes

2.2 This policy applies to all staff, volunteers, trustees, contractors, temporary workers and anyone acting on behalf of Allergy UK who processes personal data.

2.3 Compliance with this policy is mandatory. Failure to do so may result in disciplinary action and could expose the organisation to legal and regulatory consequences.

3. Definitions

3.1 For the purposes of this policy, the following definitions apply:

- "Individual(s)" - Means any person whose personal data is processed by Allergy UK, as outlined in this policy, regardless of the team or department holding that data.
- "Personal Data" - Any information relating to an identifiable living individual, as defined by UK GDPR.
- "Special Category Data" - Personal data that requires a higher level of protection under UK GDPR, including health data, genetic data, racial or ethnic origin and other sensitive information.
- "Data Controller(s)" - Refers to authorised members of Allergy UK staff who access, hold, update or otherwise process personal data on behalf of the organisation, in line with their role and responsibilities.
- "Processing" - Any operation performed on personal data, including collection, storage, , sharing, amendment or deletion.

4. What personal information do we collect and when we collect it

4.1 Personal information is information that can be used to identify a person as an individual. In the context of this policy "personal information" can be an individual's personal data. If it is a child's or someone for whom they are a carer, any personal information collected will agree with a parent or guardian. Allergy UK may process personal data such as a first name, surname, date of birth, date of death, email address, postal address, home telephone number, mobile telephone number, gender, ethnicity, marital status, photographs or videos, social media name, bank account details, credit/debit card details, next of kin details, IP address and, where a person is a UK tax payer, details so that we can claim Gift Aid where agreed. Allergy UK does not use community-provided photographs or videos to train AI systems and does not create AI-generated derivatives of real people. Images are used only in their original form except for minimal, non-altering edits (e.g., cropping, lighting adjustments). These rules follow the safeguards set out in our AI Policy and Safeguarding Children Policy.

4.2 Where images are published online, users should be aware that third-party AI companies may scrape public websites to train AI systems (e.g. automated extraction of data from websites) which is beyond Allergy UK's control.

4.3 Personal data is stored as outlined in 10.5 of this document. We may also collect special categories of data, as detailed below.

We may collect personal information when a person:

- uses our Helpline telephone service.
- uses our Helpline webchat service;
- signs up for our Allergy Alerts service;
- uses our website;
- downloads a Factsheet from our website;
- orders products and services from us (such as translation cards);
- makes a donation to us;
- tells us about a fundraising event they are organising or taking part in;
- registers for a place at one of our fundraising events;

- asks about our activities or for us to send them something about our services;
- registers for one of our events;
- attends an event or exhibition not organised by us and agrees with the organisers that they can supply us with their personal information;
- enquiries about signing up for one of our product endorsement schemes;
- becomes a corporate partner;
- registers as a catering venue for our food safety scheme;
- registers as a school for our schools' information projects;
- signs up to receive our newsletter;
- signs up to receive our publications;
- enters a prize draw or competition on our website or social media channels;
- fills out a survey or questionnaire;
- asks for press statements or requests from a media spokesperson;
- uses one of our social media channels such as Facebook, Twitter, LinkedIn and YouTube and asks us a question, requests something from us, or sends us a direct message;
- supplies personal details to be in the public domain or via a publicly accessible source, such as the website of the company they work for or on LinkedIn;
- applies for a bursary;
- apply for a job with us;
- becomes a supplier;
- volunteers for us;
- or otherwise provides us with their personal information through other means.

4.4 The following list identifies the kind of data that that we will process, and which falls within the scope of "special categories" of more sensitive personal information:

Equality Purposes

There may be specific equality laws or other legitimate purposes which require us to hold on-file categories of information which relate to equality data. This data will be kept on file with the consent of each individual and used solely for the purposes of statistical data required for monitoring equality of opportunity and treatment across all employees and/or volunteers. For example, age, disability, gender, gender reassignment, race, religion or belief, and sexual orientation to encourage compliance with the Human Rights Act.

Health Data

If a person tells us about a health/medical condition or experiences and symptoms of allergy when using services or takes part in an event we will make it clear to them, at that time, what information we are collecting and how we will use the data.

Genetics, Race and Ethnic Origin Data

We participate in research activities that are associated with understanding allergic disease. Allergy UK may be the lead for a research project, or we might partner with other associated organisations. Research evidence has shown that genetics, race and ethnic origin can be factors involved in allergy. We would only use identifiable personal data where explicit consent has been provided in advance. Anonymised data might be used. When collecting information specifically in respect of a particular research project we will make it clear why we are collecting data and how the data will be used.

Finance Data

If a person uses their credit or debit card to donate to us, buy something or pay online or over the phone, we will ensure that this is done securely and in accordance with the Payment Card Industry Data Security Standard (PCI DSS). We do not store credit or debit card details following the completion of a financial transaction. All card details and validation codes are securely destroyed once the payment or donation has been processed. Only those staff authorised to process payments will be able to see card details.

5. Why we collect and how we use personal information

5.1 We may collect personal information for several reasons, such as:

to provide a person with appropriate clinical advice when they get in touch with us, where appropriate, throughout the lifetime of their medical condition(s) and their ongoing contact with us;

- to protect their vital interests, in the case of life-or-death situations;
- to comply with legislation and regulations;
- to enter a contract with them or take steps to enter a contract with them;
- to provide them with the services, products and/or information which they have signed up to or requested;
- to process any donation, we may receive from them;
- to ask them to help us raise money or donate money to our charity;
- to respond to a question or enquiry;
- to register a person for a fundraising event, where we have bought a place, and to send them details about that event and how to send us the money raised and collected;
- to keep a record of a person's own fundraising event for us;
- when a person makes use of one of our specialist clinical services;
- to invite participation in surveys and research to use the results for statistical analysis to help improve our services and gather statistics on areas relating to allergic disease in the UK;
- to be a case study for us, where we may also use photos or a video on our website or other channels, with consent;
- for internal record keeping, such as the management of feedback or complaints;
- to maintain a list of people who have explicitly told us that they do not want us to contact them;
- to analyse and improve the services we offer;
- or to set a person up on our systems as, for example, a bursary recipient or a volunteer.

5.2 **Use of Clinical Documentation Tools (Heidi Health)**
Allergy UK may use Heidi Health, a secure third-party clinical documentation platform, to support clinicians in recording consultations and generating clinical notes and reports. This may involve the processing of personal data, including special category health data, where necessary to provide clinical advice and services. All use of Heidi Health is conducted in accordance with UK GDPR requirements, and appropriate safeguards and data processing agreements are in place to ensure the confidentiality, integrity and security of personal data

5.3 Once collected, we may anonymise your data for activities relating to our legitimate interests, such as being able to collate statistical data to inform our services, survey data or research.

5.4 We aim to ensure that all information we gather about a person is accurate and kept up-to-date.

If any of the information we gather about a person is inaccurate and either they advise us or we become otherwise aware, we will ensure it is amended and updated as soon as possible.

5.5 We may contact a person for direct marketing purposes by post, email, home telephone, mobile telephone or text, if they have given us permission to do so. We will only contact a person for the purpose requested via the channel they request. For example, if a person only wishes to receive our newsletter, we will only send emails about this. It is each person's choice about the type of communication and information they receive from us.

5.6 We will not use personal information for direct marketing purposes if a person has asked us not to do so. However, we will retain details on a suppression list to help ensure we do not contact them. A person may ask for any personal information about them that we hold to be deleted and destroyed at any time but please note, in that case we will have no record of any marketing preferences. There may also be times when we cannot delete data because of other laws or regulations. We will inform a person, if possible, if data cannot be deleted.

5.7 We use several third-party data processors to process your data and have agreements in place to ensure that they comply with the necessary standards. The list of these third-party data processors can be found in section 10 of this Privacy Policy, as updated from time to time.

6. Use of Artificial Intelligence (AI)

6.1 The BAF uses Microsoft Copilot as its Artificial Intelligence (AI) tool and Microsoft Teams transcription to support internal administration, content drafting, and productivity. These tools operate strictly within Allergy UK's secure Microsoft 365 environment and follow UK GDPR requirements

6.2 AI is not used to make decisions about individuals, analyse symptoms, assess risk, provide clinical judgement, undertake profiling, or influence any safeguarding decisions. All decisions that affect individuals are made by trained staff.

6.3 The BAF does not use community-provided photographs or videos to train AI systems. We do not generate AI-altered representations of real people. Images featuring children, young people, or vulnerable adults are handled in accordance with our Safeguarding Children Policy and our AI Policy. Please be aware that images published publicly online may be scraped by external AI systems beyond our control.

6.3 Personal data and special category data are never entered into public or non-approved AI systems, and The BAF prohibits staff from using external generative AI tools (e.g., free versions of ChatGPT, Bard, Midjourney) for any processing of personal information. This ensures that personal information is not exposed to systems outside the control of The BAF.

6.4 Where Microsoft 365 AI features (e.g., Copilot) process personal data temporarily to generate outputs, this processing remains within The BAF's Microsoft tenant, is protected by enterprise-grade security controls, and is used solely to fulfil the task requested.

6.5.1 Allergy UK may use approved third-party clinical documentation tools, such as Heidi Health, to support authorised clinical staff in recording, transcribing, and generating clinical notes or reports. Any use of such tools is subject to appropriate data protection safeguards, contractual controls, and compliance with UK GDPR. Personal and special category data processed through these tools is limited to what is necessary for clinical purposes, is accessed only by authorised personnel, and is handled in accordance with this Privacy Policy and our Information Security Policy.

7. Our legal basis for processing and storing personal data

7.1 The BAF uses certain automated digital tools, such as webchat systems, website analytics, and Microsoft Teams transcription, to support communication and service delivery. These tools may process personal data to provide requested services (e.g., recording a webchat, transcribing a meeting) but do not make automated decisions about individuals. All outputs are reviewed by staff, and no automated profiling or assessment takes place.

7.2 Our legal basis for processing and storing personal data differs depending on when and why a person has provided us with their personal information. For example:

For the purposes of health care advice and to protect a person's vital interests

- If a person supplies us with details of personal information relating to health or medical conditions(s), whether over the phone or on our Helpline, via our webchat service, by signing up to Allergy Alerts, or via another method, we will record and store these details for the purpose of providing health care advice. The data input is always undertaken by a health
- professional or by someone who is subject to an equivalent duty of confidentiality. This is to protect the person's interests and always provide them with the most appropriate clinical advice and information when they contact us. Only individuals involved in our clinical service have access to this information.
- When a person calls our Helpline service or any other service at the BAF, the caller is notified prior to speaking to someone that the call is recorded. t This is because we provide clinical advice, through a health professional, on our Helpline. If, later, our advice is questioned, a person does not follow our advice or raises a dispute or complaint, then we need to ensure that we have a record of the conversation. In those situations, we will therefore record the call for the purpose of providing health care advice. There may also be times when either the person who calls our Helpline, or the person about whom they are calling may be in danger or we are provided with information which we believe may indicate there is a need to enact safeguarding procedures. In these circumstances, we have a legal duty of care to collect personal data to protect the person's vital interests and, if necessary, this may include passing details on to the emergency services or other relevant authorities.

8. Consent

- Collection of details of health and medical data which is not related to the purpose of the provision of health care advice or protecting a person's vital interests will be based on the person's consent. Section 12 provides further details on individual rights.
- We may contact those included in our database to raise awareness of research projects which are seeking participant involvement. This activity may require some profiling to try to ensure that only people for whom it may be relevant are contacted.

8.1 **For the performance of a contract or to take steps to enter a contract**

- If a person sets up a direct debit to donate money to us regularly, orders translation cards from us, is representing a company that wishes to work with us, either by signing up to one of our endorsement schemes or working with us as a partner or a supplier, or for another reason, we will collect personal information to allow us to take steps to enter into a contract.

8.2 **Direct Marketing**

- Consent for us to process and store personal information is separate from giving us consent for direct electronic marketing purposes, which is when a person has requested that we send by email or other electronic method, from time to time, marketing or other materials promoting our organisation and charitable aims. We always ask for separate consent for electronic direct marketing purposes to make it explicitly clear as to what a person is consenting to and how we will be using personal information. For example, we may email you information concerning research projects which are looking for participants. This activity may require some profiling to try to ensure that only people for whom it may be relevant are contacted.
- If we have processed and stored personal data and a person has provided us with consent to contact them by opting in to receive direct marketing by email from us then, every 12-24 months, we may ask them to verify the personal information we hold about them and provide us with their consent to continue to receive direct marketing from us. We do this
- To ensure the personal information we hold on them and their preferences for any contact from us is as accurate and up to date as possible.
- We may also send direct marketing information by post, using the postal address we have on record for supporters, unless they have opted out from receiving such information. Our legal basis for such direct marketing is that it is in our legitimate interests to raise the profile of our charity and provide information in line with our charitable aims, including events, projects and requests for donations.

9. Data Protection and Security

9.1 We take steps to ensure all information is safe and secure, and that all staff are aware of and comply with their responsibilities in relation to data protection legislation. A copy of our Information Security Policy can be accessed through the BAF HR department. We will ensure that:

- The Information Security policy is up to date
- All staff undergo training in data protection requirements
- Access to personal data is based on role responsibility and a 'need to know' basis, which is seen as good practice by the Information Commissioner's Office (ICO). We do this to reduce the risk of inappropriate access to personal data by staff or volunteers.
- Access to our office is through use of secure keypad entry and the code is changed regularly as required.
- We have confidential waste processes in place in the form of a shredder. This improves the security of documents which may contain personal data which is no longer required.
- We have formal retention schedules in place to ensure that we only keep personal information for an appropriate length of time.
- We have security locks for our I.T. screens.
- We enforce regular password changes through our IT systems.
- We have a clear desk policy about personal information – nothing containing personal information is to be left out on a desk outside office hours.
- All paper files or discs containing personal information are held in securely locked cabinets, with only the appropriate staff having access to them.

9.2 Although we cannot fully guarantee the security of any information transmitted to us, we enforce strict procedures and security features to protect all information and prevent

unauthorised access.

10. Storing information and how long we store it

10.1 We only hold personal information for appropriate lengths of time, in line with the organisational Data Retention Policy and will contact a person for consent to continue holding or destroying the data.

10.2 We take into consideration our legal obligations, the guidance of relevant UK authorities such as the Information Commissioners Office, the National Health Service, Fundraising Regulator and tax and accounting bodies, when determining how long we should retain information.

10.3 **Heidi** **Health**
Purpose: Clinical documentation tool used by authorised clinical staff to record, transcribe, and generate notes and reports from patient interactions
Further Information: https://www.heidihealth.com/en-gb/legal/privacy-policy

10.4 When we no longer need to retain personal information, we will ensure it is securely deleted and destroyed at the appropriate time, unless a person provides consent for us to retain it for a further period.

11. Our websites and cookies

11.1 Our websites use Google Analytics to track what a visitor sees on our website, and which pages they visit. We use this data to determine the number of people using our site, to better understand how they find and use our web pages, and to see their journey through the websites.

11.2 Although Google Analytics records data such as geographical location, the device being used to access our website, internet browser, and operating system, it does not personally identify any person. Google Analytics also records a computer's IP address, and although this could be used to personally identify a person, Google does not grant access to this.

11.3 Our websites contain links to other websites belonging to third parties and we sometimes choose to participate in social networking websites including but not limited to Twitter, YouTube, LinkedIn, and Facebook. We do not have any control over the privacy practices of these other websites or applications. It is a person's individual responsibility to make sure when they leave our website that they have read and understood that website's privacy policy in addition to our own.

11.4 We also use cookies to monitor the usage of our websites and webchat communications, to help the websites work well and to track information about how people are using them.

12. Information sharing, disclosure, and third-party data controllers and data processors

12.1 We will not share a person's information with any third party apart from trusted partners we work with to help deliver our services.

12.2 We require all our trusted partners to comply with data protection regulations and our standards, and we allow them only to process information in strict compliance with our instructions. We will always make sure appropriate contracts and controls are in place and we regularly monitor all our partners to ensure their compliance.

12.3 We may disclose personal information to third parties if we are required to do so through a

legal obligation, to enable us to enforce or apply our terms and conditions or rights under an agreement or to professional advisers, to protect us, for example, in the case of suspected fraud or defamation.

12.4 We may use third parties to process personal data on our behalf. Some of these third parties have servers located outside the EU, which means that when a person uses these services, data is passed between the UK and a country outside the EU. We will take steps to ensure privacy continues to be protected as per UK data protection legislation in line with the BAF Information Security Policy.

12.5 These third parties have been carefully chosen and all commit to complying with the legislation set out in section 1 of this Privacy Policy. Some of these parties are based in the USA and confirm that they have adopted the new Standard Contractual Clauses (SCCs) as per GDPR – EU Commission requirements

12.6 Microsoft is listed as one of our data processors. This includes the use of AI enabled productivity features within Microsoft 365 (e.g., Copilot), Teams which process data in strict compliance with Microsoft's enterprise security and privacy standards. All processing occurs within Allergy UK's Microsoft tenant and aligns with our AI Policy and Information Security Policy.

12.7 Some of these partners, including clinical documentation providers such as Heidi Health, may process special category health data on our behalf where required to deliver clinical services.

Company	Purpose	Further Information
Microsoft	Organisational IT operating system	https://privacy.microsoft.com/en-gb/privacystatement
Heidi Health	Clinical documentation platform used to record consultations and generate clinical notes/reports	https://www.heidihealth.com/en-gb/legal/privacy-policy
BT Business	phone service provider	https://business.bt.com/privacy-policy/
I.T. Support (UK) Ltd	external contractor to provide I.T. support	Privacy Policy
Salesforce	logging business and stakeholder information.	Privacy Policy
Doodle Poll	To support a project and the arrangement of appointments	https://doodle.com/en/privacy-policy/
Allergy UK Website:	WordPress – content management system	https://automattic.com/privacy/

	for the website Fat Beehive – website provider Google –to track movements for the website	https://www.fatbeehive.com/privacy-notice/ Privacy Policy
Financial services to process payments	• Elavon Digital Europe Ltd • T/A Opayo – a payment processing service • CardSave/World Pay – payment processing system • Donr (text to donate)	https://legal.donr.com/supporter-privacy-policy
Social Media	• Hootsuite- social media management platform • Meta (Facebook/Instagram • Twitter/X L • LinkedIn	https://www.hootsuite.com/en-gb/legal/privacy https://www.facebook.com/privacy/policy/ https://twitter.com/en/privacy https://www.linkedin.com/legal/privacy-policy

13. Changes to the privacy policy

13.1 This Privacy Policy replaces all previous versions and is correct as of February 2024.
Our Privacy Policy may change from time to time. We will post any Privacy Policy changes on the website https://www.allergyuk.org/privacy-policy/ . If the changes are significant, we will provide a more prominent notice. We will also keep prior versions of this Privacy Policy in an archive and for information purposes only. Future updates may include changes relating to the safe and transparent use of emerging technologies, including Artificial Intelligence. A person can request to see the version of the Privacy Policy they signed up to at any time by contacting us at info@allergyuk.org . The most recent version will supersede all previous versions and we advise people to check our pages periodically.

14. Your rights as an individual

14.1 Under data protection legislation, a person has the right to:

- request information about any automated tools used to process your data, including AI□assisted systems, and to ask for clarification about how such tools operate within Allergy UK.
- obtain confirmation from us about whether we are processing their personal information, how, and why;
- request that we update or amend the information we hold about them, if it is wrong;
- object to the processing of their information for direct marketing purposes or profiling;
- object to their personal information being subject to automated processing;
- request a copy of the information we hold about them;

- change their communication preferences at any time;
- ask us to remove their personal information from our records without delay;
- a right to portability of photographs and images which they provided to us, returned in a 'machine readable' format and, where requested, transferred directly to another data controller (free of charge);
- raise a concern or complaint with us about the way in which their information is being used.
- if dissatisfied with the outcome of any complaint we have investigated, then raise a concern or complaint about the way in which their information is being used with a data protection authority. In the UK, the data protection authority is the Information Commissioner's Office (ICO) who can be contacted at https://ico.org.uk/.

If at any time a person contacts us regarding any of their rights above, we will respond to their enquiry within ten working days.

15. Contacting us

If a person would like us to contact us in relation to this Privacy Policy and our processing of personal information, then please contact us via email on info@allergyuk.org or by post at: Data Protection, Allergy UK, London House, Texcel Business Park, Thames road, Crayford, DA1 4SL

16. Associated Policies

Complaints

Data Protection Records Retention

Safeguarding Children & Young people

Safeguarding vulnerable adults

Subject Access Request

Data Breach

Webinar Privacy Policy