

Privacy statement

As one of the UK's leading and longest-standing charities for children and young people, the National Children's Bureau is proud to champion change across the UK to make childhood better.

By gathering and analysing evidence, by listening to children's experiences and by getting organisations to unite in pursuit of shared goals, we're able to influence legislation and drive changes right across the system to make things work better for children and communities.

We build partnerships and train those who work directly with children, young people and families, to make sure the changes are long-lasting.

Keeping people informed and connected on the issues children are facing is a key part of what we do, and we've always done that with care, and with a strong commitment to privacy and security.

Under the **UK GDPR** (Data Protection Act 2018 "DPA" and EU Directive 2016/680 and Regulation EU/2016/679 – 'The General Data Protection Regulation' "EU GDPR") our Privacy Statement explains how we handle, store, retain and use your data. This policy sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our views and practices regarding your personal information and how we will treat it. In compliance with the UK GDPR, we are making it easier for you to understand how we use your data through greater transparency, particularly but not limited to:

- 1 [How we collect your data?](#)
- 2 [How and where does NCB store my data?](#)
- 3 [How does NCB use my data?](#)
- 4 [How long does NCB retain my data for?](#)
- 5 [Does NCB share my data with other relevant professional bodies/other third-parties?](#)

- 6 [What are my rights?](#)
- 7 [Children, young people and vulnerable adults](#)
- 8 [Accountability and governance](#)
- 9 [Data protection breach](#)
- 10 [Updating our Privacy Policy](#)

For the purpose of the UK GDPR the data controller is the National Children's Bureau, registered with the Information Commissioner's Office (registration number Z7988835) registered charity No. 258825, registered in England and Wales No. 952717, registered office: National Children's Bureau, 23 Mentmore Terrace, London E8 3PN. NCB is a company limited by guarantee.

NCB is registered with Cyber Essentials, Certificate No: 4180798

[1. How we collect your data](#)

Personal data we hold about you may include your name, email address, postal address, telephone or mobile number, date of birth, financial details, and credit/debit card information. We may also hold information from when you have participated in a survey for our research purposes, attended one of our training events, provided us with feedback on our services and events, subscribed to our newsletters, subscribed to on-line forums we administrate, and from when you have visited one of the NCB Family's websites. Our websites are:

The National Children's Bureau www.ncb.org.uk

The National Children's Bureau Northern Ireland www.ncb.org.uk/northern-ireland

The Anti-Bullying Alliance (ABA) www.anti-bullyingalliance.org.uk

The Northern Ireland Anti-Bullying Forum (NI ABF) www.niabf.org.uk / www.endbullying.org.uk

The Childhood Bereavement Network (CBN) www.childhoodbereavementnetwork.org.uk

The Council for Disabled Children (CDC) www.councilfordisabledchildren.org.uk

The Lambeth Early Action Partnership (LEAP) www.leaplambeth.org.uk

National Bereavement Alliance www.nationalbereavementalliance.org.uk

Plan if www.planif.org.uk

Learn Equality, Live Equal learnequality.virtualdisplayboard.org.uk

It is important to note that if you are a member of one (or more) of our Special Membership Groups or other forums and when you visit one of our websites that the information we collect about you is processed by The National Children's Bureau as the registered charity and data controller.

When you do visit one of our websites, the following information will automatically be collected:

Technical information, including the Internet protocol (IP) address used to connect your computer to the Internet, your login information, browser type and version, time zone setting, browser plug-in types and versions, and operating system and platform;

Information about your visit, including the full Uniform Resource Locators (URL), clickstream to, through and from our site (including date and time), products you viewed or searched for page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page.

Information we receive from other sources. This is information we receive about you if you use any of the other websites we operate or the other services we provide. In this case we will have informed you when we collected that information if we intend to share that data internally and combine it with information collected from you. We will also have told you for what purpose we will share and combine your information. We work closely with third parties including, for example, sub-contractors in technical, payment and delivery services. We will notify you when we receive information about you from them and the purposes for which we intend to use that information.

Cookies

Our websites use cookies to distinguish you from other users. This helps us to provide you with a good experience when you browse one of our website and also allows us to improve our sites. For detailed information on the cookies we use and the purposes for which we use them see our [Cookie policy](#).

Lawful basis for NCB to collect and process your personal data

There are six available lawful bases for processing your personal data under the UK GDPR. In compliance with the overarching principles of the UK GDPR, particularly

in terms of transparency, we will determine our bases for processing your personal data in-line with NCB's purpose and our relationship with you. We shall determine our lawful bases in-line with criteria set out under the UK GDPR and we shall record our bases on NCB's Data Asset Register and any corresponding records. The six lawful bases are:

A. Legitimate interests

We will collect and process your personal data under 'legitimate Interests', proportionately and balanced to fulfil our organisational purpose. Our reason for using this basis will be considered either to be in your or our interests, commercial interest or wider societal benefit. We will ensure that we use your data under this basis only in ways that you may expect and that are easily explainable such as marketing, events, training, or if you participate in any of our many advisory or working groups and forums.

B. Contract

We will collect and process your personal data under the legal basis of 'Contract' to fulfil our contractual obligations to you, including during procurement or other such processes leading up to entering into a full contractual agreement with you.

C. Legal Obligation

We will collect and process your personal data under 'Legal obligation' where we have to do so to comply with a common law or statutory obligation laid down by UK or EU law. This includes where we are legally required to comply with statutes set out by regulatory bodies including Companies House and the Charity Commission.

D. Consent

Your consent for us to collect and process your data must be unambiguous and involve a clear affirmation action (Positive Opt-in) and specifically bans pre-ticked opt-in boxes. All of our materials, such as newsletters you may sign up for via our websites, comply with this and demonstrates how we wish to maintain your trust and your engagement with us through providing you with real choice and control as to what information you receive from us, how we contact you and subsequently process your data. We shall also document accordingly your consent you have provided, how and when you provided it, and the information we have provided you with regard to your consent. This will include clear information as to how you may withdraw your consent at any time and make this a smooth and easy process for you to do so. We will also advise you as to how and when we may contact you, if applicable, to either reconfirm or update your consent. We will periodically

review our Consent Policy and Consent Forms to ensure they remain compliant in-line with any future amendments or requirements under the GDPR and advise you of any changes we may make.

E. Vital interests

We will collect and process your personal data under 'Vital interests' should we need this data to protect your life, within the limited scope that generally only applies to matters of life and death. We will not use this basis for collecting data that falls under a Special Category (please see G, below) where we are required to obtain consent.

F. Public task

We will collect and process your personal data under 'Public task' should we need this data to carry out a specific task in the public interest which is laid down by law. This may apply to processing of personal data that is necessary for statutory or governmental functions or in the administration of justice.

Owing to the nature of NCB's purpose; our programme delivery; our position as a highly trusted partner and convener; our direct participation work with children, young people and those who support them; our work with practitioners; and our extensive research that enables us to inform policy, we anticipate that the majority of our legal basis will come under Legitimate Interests, Contract and Consent.

Notwithstanding, and to maintain your trust in us, we will always consider the other three bases and apply them should they be deemed the most appropriate with regards to your relationship with us.

There are two further subcategories under personal data that we may need to collect at times:

G. Special category data

We will collect and process your personal data under 'Special category data', under Article 6, where this information is more sensitive and, as such, so we can further protect your fundamental rights and freedoms. Such data may, but not necessarily, have an obvious link to another data category, particularly Consent or Vital Interests. There are currently ten types of Special Category Data set out:

race;

ethnic origin;

politics;

religion and philosophical beliefs

trade union membership;

genetics;

biometrics (where used for ID purposes);

health;

sex life; or

sexual orientation.

H. Criminal offence data

We shall only collect and process your personal data relating to Criminal Offence Data under particular safeguards set out in the GDPR, Article 10, that relate to criminal convictions and offences, or related security measures. We recognise that we are not permitted to keep a comprehensive register of criminal convictions unless they are required under the control of official authority.

2. How and where we store your data

The personal information that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). We will take all steps reasonably necessary to ensure that your information is treated securely and in accordance with this privacy policy. We will not transfer your personal information to a country outside of the EEA unless we are satisfied that we are entitled to do so pursuant to the requirements of the UK GDPR.

All information you provide to us is stored securely and any payment transactions will be encrypted using SSL technology. Where we have given you (or where you have chosen) a password which enables you to access certain parts of our site, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal information, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

3. How we use your data

We use your personal data we have collected from and hold about you in the following ways:

to carry out our obligations arising from any contracts entered into between you and us and to provide you with the information, products and services that you request from us;

to provide you with information about other goods and services we offer that are similar to those that you have already purchased or enquired about and, in so doing, will give you the opportunity to positively opt-in;

to notify you about changes to our services;

to ensure that content from our websites is presented in the most effective manner for you and for your computer.

to administer our sites and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;

to improve our sites to ensure that content is presented in the most effective manner for you and for your computer;

to allow you to participate in interactive features of our services, when you choose to do so;

as part of our efforts to keep our sites safe and secure;

to measure or understand the effectiveness of any advertising we serve to you and others, and to deliver relevant advertising to you;

to make suggestions and recommendations to you and other users of our sites about goods or services that may interest you or them;

to work on campaigning and influencing government policy;

to share the findings of our research and public policy analysis;

to request donations to fund our work;

to invite people to attend events about developments in the children's sector;

to distribute information about our chargeable products and services.

4. How long we retain your personal data

We commit to retaining your personal data for no longer than is necessary and in-line with legal minimum and maximum requirements which are clearly set out in

our Retention Policy. As feasible, we will erase your personal data as soon as possible; for example, if you have signed up to attend one of our events we shall delete most of the personal information you have shared with us once that event has taken place.

Where it is appropriate for us to retain information such as feedback from one of our events, surveys and research purposes the data we collect will be anonymised. As such, we shall only retain the details and statistics needed to support us in our organisational purpose to continue making improvements for children, young people and all those who support them.

As with all our processes and practices, we will ensure all our staff have a comprehensive understanding of our Retention Policy and to ensure any changes to it are communicated efficiently. Similarly, we will have mechanisms in place so all of our delivery partners and other third party processors understand our Retention Policy and commit to our expectations of their treatment of your personal data.

To maintain your trust and confidence in us, our updated Retention Policy will be available here soon. Should you have any queries about our Retention Policy, our Data Protection Officer will be very happy to help: DataProtection@ncb.org.uk

5. How we share your data with other relevant professional bodies/other third parties

We are committed to only sharing the personal data we have collected from you with third parties as and when required in-line with our organisational purpose and in delivery of our programmes, projects, training and other events, research purposes. We will ensure our delivery partners and third-party processors fully understand and commit to complying with the agreements they enter into with us as to how they treat your personal data, including how it is stored and for how long it is retained. If you have any queries please contact our DPO at DataProtection@ncb.org.uk

We will disclose your personal data to third parties:

if the National Children's Bureau or substantially all of its assets are acquired by a third party, in which case personal data held by it about its customers will be one of the transferred assets;

if we are under a duty to disclose or share your personal data in order to comply with any legal obligation, or in order to enforce or apply an agreement; or to protect the rights, property, or safety of the National Children's Bureau,

our customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection.

6. Your rights

Your right to be Informed

Your right to be informed about the collection and use of your personal data is a key transparency requirement under UK GDPR. NCB commits to this by providing information regarding the purpose we process your personal data, our retention periods for that data and who it may be shared with. We will be reviewing all such documentation to ensure this information is concise, transparent, intelligible, and easily accessible with links to related policies or guidelines. To maintain your trust in us, we will periodically review our privacy information and provide notification of any substantive amendments.

Your right to be forgotten (also referred to as right to erasure)

You have the right to be forgotten (to have your personal data erased or to stop the processing of your data) though this is not absolute, it relates particularly, but is not limited, to when:

Your personal data is no longer necessary for the purpose we originally collected it for;

Our lawful basis for holding your data was through Consent and you wish to withdraw consent;

Our lawful basis for holding your data was under Legitimate Interests, your circumstances have changed so this no longer applies;

We have to anonymise or erase your personal data in-line with our Data Retention Policy.

We will respond to you without undue delay and within one month calculated from the day following receipt of your request (consideration applied to bank holidays). Requests are to be made in writing and satisfactory identification will need to be provided. There is generally no fee for you to exercise your Right to be Forgotten unless, we consider it manifestly unfounded or excessive but still decide to comply with your request where we shall apply a reasonable fee to cover administrative costs.

Your right to rectification

You have the Right to Rectification should you consider we have collected inaccurate or incomplete personal data on you. The latter may involve a supplementary statement to the incomplete data. You may make a request for rectification verbally or in writing and we will respond to you without undue delay and within one month calculated from the date following receipt of your request (consideration applied to bank holidays).

Your right to data subject access

You have the right to data subject access to your personal data and any supplementary information we may have collected. This allows you to be aware of and verify the lawfulness of our collection, retention and processing of your information. You have the right to obtain from us:

- confirmation that your data is being processed;
- access to your personal data;
- other supplementary information

Data subject access requests are to be made in writing and appropriate identification will be required. We will generally provide you with your information in a commonly used, secure, electronic format, but we will endeavour to meet any other format you may require. In the instance that we process a large quantity of your information, we are permitted under the UK GDPR to ask you to specify further as to what information your request relates to.

If we receive a request from you, we will respond without undue delay and within one month calculated from receipt of your request (consideration applied to bank holidays). However, should your request be particularly complex or numerous, under UK GDPR we have the right to extend the response period. Under such circumstances we will inform you of the extension within the first month from when your request was received and explain why we feel the extension in your best interests.

Under UK GDPR we can refuse to comply with a Subject Data Access request, should it be manifestly unfounded or excessive including if the request is repetitive in nature. Under such circumstances, we will provide you with sound justification of our decision with undue delay and within one month calculated from the day following your request (consideration applied to bank holidays). While it is unlikely that we would refuse such a request, should this situation arise we will remain committed to providing you with further support and inform you as to your right to make a complaint to the ICO (or other relevant supervisory authority). We will provide you with a copy of the information you request free of charge.

However, under UK GDPR, we may charge a reasonable fee if the request is manifestly unfounded, excessive, repetitive or for requests for further copies of the same information.

Our Data Subject Access Policy and Request form will be available here soon. In the meantime, if you have any queries please contact our DPO.

Your right to data portability

Your right to data portability allows you to obtain and reuse your personal data for your own purposes across different services, to move, copy or transfer your data from one IT environment to another in a safe and secure way without hindrance. Your Right to Data Portability only applies to NCB:

when you have provided us with your personal data in our capacity as a controller;

where you have given us your consent to process your data;

where we process your data for the performance of a contract.

Our updated Data Portability Policy will be available here soon. In the meantime, if you have any queries please contact our DPO.

Your right to object

You have the right to object, on grounds relating to your particular situation, to us collecting and processing your personal data if:

our processing is based on legitimate interests of the performance of a task in the public interest/exercise of official authority (including profiling);

we use your data for direct marketing (including profiling);

our processing is for purposes of scientific/historical research and statistics.

Should you exercise your right to object, we will stop processing your personal data unless we can demonstrate compelling legitimate grounds that override the interests, rights and freedoms of an individual or if the processing is for the exercise of defence of any legal claims.

This does not apply to your Right to Object to us processing your personal information for direct marketing where there are no exemptions or grounds for us to refuse your request. If we receive such a request from you, we will deal with your objection without undue delay and free of charge.

If, however, we are conducting research where the processing of your personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing.

Your right to positively opt-In or unsubscribe

We will always meet your right to positively opt-In through appropriate means, such as preferences that require your affirmation. You can unsubscribe from any of our newsletters, bulletins or other mailing lists at any time and we shall continue to make this obvious and easy for you to do.

If you have any queries with regard to your rights, as outlined above, or to make a particular request, our Data Protection Officer will be very happy to help:

DataProtection@ncb.org.uk

For further information on Your Rights, please visit:

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>

7. Children, young people and vulnerable adults

Owing to the nature of our purpose, we have particular measures in place to protect the rights and freedoms of children, young people and vulnerable adults as to why and how we collect, process, store and retain their personal data. While the UK's age limit for obtaining parent/guardian consent to collect such data is 13, as we are highly committed and sensitive to safeguarding measures we have taken an organisational decision to set the age limit at 16. We therefore require joint Parent/Guardian and Young Person consent for 13 to 16 year olds. In the instance where a young person is over the age of 16 and there is a reasonable belief that they do not have capacity to consent to an activity as defined under the Mental Capacity Act 2005 we also require joint Parent/Guardian and Young Person consent.

Under all lawful basis for collecting and processing personal data we will ensure that the child, young person or vulnerable adult can fully understand what they are consenting to, what they may be agreeing to in entering into a contract.

Where we may deem legitimate interest as our lawful basis, we will identify any potential risks in collecting and processing such personal data and ensure that age appropriate safeguards are in place.

8. Accountability and governance

At NCB, we have robust accountability and governance frameworks across all of our activities. This has included us putting in place additional mechanisms to update our data protection processes to ensure we are protecting your personal data, fundamental rights and freedoms in compliance with new regulations under the UK GDPR. These updated or newly implemented processes include:

Contracts

We periodically review and ensure that our contracts and data processor agreements clearly set out our and our processors responsibilities and liabilities. This will include our processors agreeing to only act on the documented instructions as issued by us and in-line with their direct responsibilities.

Documentation

We periodically review what, where and why we are holding personal data, including the legal basis, if data is shared with third parties and the data retention limit. This information is collated and held in our organisational Data Asset Registers that are periodically reviewed and updated.

Data protection impact assessment

We will undertake a data protection impact assessment where we consider there could be potentially high risk with regard to processing personal data, such as complex projects particularly where personal data may be shared with third parties. Our DPIA will cover the nature, scope, context and purpose of processing data; the necessity, proportionality and compliance measures; and, will enable us to assess potential risks to individuals and how to mitigate and monitor any such risks.

Data protection breach register

Our Data Protection Officer maintains an organisational Data Protection Breach Register to record any incidents where the protection of data has been compromised.

How we protect your personal data

We always ensure that the means by which we process and store your personal data is done so securely by appropriate technical and other organisational measures relating to confidentiality, integrity and availability of our systems and processes and we periodically assess our IT security with our IT provider. With our commitment environmental issues, we work in an ever more paper-less way; but, where data may need to be kept in hard-copy we ensure it is under secure filing or other relevant means. Our security measures include ensuring our staff and third-

party processors have sound understanding of risks that may result in accidental loss or theft of data and the measures we have in place to mitigate such risks, for example, use of USB sticks limited to only when absolutely essential.

Reporting to our Board of Trustees

Our Board has an identified Data Protection Lead Trustee which fulfils the purpose of a direct line for our DPO to Board level. Our Board and the Finance Risk and Audit Committee (FRAC) have standard and recurrent agenda items that monitor our continued compliance across all key governance areas.

9. Data protection breach

We will continue to maintain all of our mechanisms, processes and controls to optimum standards as proportionate to our organisational purpose and extent and nature of our activities. We have robust breach identification, investigation and internal reporting procedures within our accountability and governance frameworks, and we will also ensure that our staff and Data Processors have sound understanding of what constitutes a Data Protection Breach and how to report any incident to our DPO efficiently. Should a breach be reported, our DPO will investigate further particularly to ascertain if the breach is high risk and if it needs to be reported to the ICO within the specified timeframe of 72 hours. If any such breach may result in a risk of adversely affecting individuals' rights and freedoms our DPO will put in motion our process of informing those individuals. Irrespective of whether the breach needs to be reported the ICO, the DPO will ensure that any breach reported is recorded on our Data Breach Register and also, as necessary, our Data Protection Lead Trustee, our FRAC and/or Board of Trustees are informed.

10. Updating our Privacy Policy

Any changes we make to our Privacy Policy in the future will be posted on this page and, where appropriate, we shall notify you by e-mail. Please check back here frequently to see any updates or changes and please do remember that our Data Protection Officer will always be happy to help if you have any queries: DataProtection@ncb.org.uk

SHARE