



1.5 Information sharing and data protection policy

Policy statement

We recognise that parents, staff, trustees, volunteers and supporters have a right to know that information they share will be regarded as confidential, as well as to be informed about how information is stored and the circumstances, and reasons, when we are obliged to share information. Information may be used by all employees in conjunction with providing our services and with Trustees when applicable with the leading and managing aspects of the charity.

The Bumblebee Children's Charity follows the data protection principles as set out under the Data Protection Act 2018. These principles state that as a charity we make sure your personal information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

We are obliged to share confidential information without authorisation from the person who provided it, or to whom it relates, if it is in the public interest. This is when:

- It is to prevent a crime from being committed or intervene where a crime may have been or
- to prevent harm to a child or adult; or
- not sharing it could be worse than the outcome of having shared it.

Where possible the decision to share information should never be made as an individual, but with the support of the trustees.

Safeguarding the welfare of our children, and vulnerable adults, is paramount in the work that we do. The three critical criteria are:

- Where there is *evidence* that the child is suffering, or is at risk of suffering, significant harm
- Where there is reasonable cause to believe that a child may be suffering or at risk of suffering significant harm.
- To prevent significant harm arising to children and young people or serious harm to adults, including the prevention, detection and prosecution of serious crime.

We will follow our Safeguarding procedures when appropriate to do so.

Storing information

The Bumblebee Children's Charity may store personal data in the following secure ways:

- As paper copies in a locked filing cabinet in the charity office.
- As electronic information on our secure IT systems in accordance with our Information technology policy.
- Children records are kept in accordance with our Childrens records policy.

Information retention

The Bumblebee Children's Charity will store personal data only for as long as it is needed.

Depending on the data it may be retained for the following periods of time:

- Operational records may be kept for up to 6 years. These records may include attendance records, medical records and registration forms.
- Other records, such as those relating to Safeguarding concerns, accidents and incidents, may be kept until the child reaches the age of 25.
- Staff employment records may be kept for up to 6 years following the cessation of employment.

Destroying information

When personal information is no longer required The Bumblebee Children's charity will destroy personal data in the following secure ways:

- Paper copies are shredded in the office on the premises.
- Electronic copies are deleted from all charity Information technology systems including hard drives, cloud storage, camera memory card and computer recycling bins.

Information sharing

People have a right to be informed and their consent to share information will be sought in most cases. The Bumblebee Children's Charity will:

- ensure parents receive information about charity policies when starting their child in the centre and they sign a registration form to say that they understand circumstances when information may be shared without their consent,
- request permission from parents before sharing information with external agencies, for example with regard to any special needs the child may have or transition to school,
- consider the safety and welfare of the child when making a decision about sharing information,

- ensure staff receive information about our policies as part of their induction process and in signing their contract of employment they say that they understand circumstances when information may be shared without their consent,
- record and report safeguarding concerns in line with our safeguarding procedures,
- ensure any information shared will be accurate and up-to-date, necessary for the purpose it is being shared for and shared only with those who need to know,
- ensure any information shared is done so in a secure way; for example via encrypted email.

Before sharing any information we will consider the following questions:

- Is there a legitimate purpose to sharing the information?
- Does the information enable the person to be identified?
- Is the information confidential?
- If the information is confidential, do you have consent to share?
- Is there a statutory duty or court order to share information?
- If consent is refused, or there are good reasons not to seek consent, is there sufficient public interest to share information?
- If the decision is to share, are you sharing the right information in the right way?
- Have you properly recorded your decision?

Data breach

A data breach can take many forms such as the loss or theft of data, the unauthorised access to, use of, or modification of data, or something apparently less direct such as equipment damage, human error, or the loss or theft of equipment. Data breaches, whether suspected or actual, will be reported to the chairperson of the trustee board. In line with our data breach procedures, as set out in the staff handbook, initial steps will be taken to determine the full particulars of the breach, working out what needs to be done to resolve and remedy the situation properly, and establishing who needs to be notified. At the early stages, this might include the police if equipment or records have been stolen. A full investigation and assessment of the breach will go into more detail, determining who will be affected by the breach and to what degree, how much data is involved, how many data subjects will be affected, the consequences of the breach and more. Some personal data breaches must be notified to the Information Commissioner's Office (ICO) and to the individual data subjects whose data is involved in the breach. In some cases, only the ICO needs to be informed, and in other cases, nobody does. Once the breach itself is resolved and all necessary parties notified, steps will be taken to prevent similar breaches from occurring in the future.

Misuse of personal information

The Bumblebee Children's Charity encourage parents/carers and supporters to discuss concerns with us. If you think your data has been misused or that it has not been kept securely please notify our administrator in the first instance. Anyone unhappy with the response from the charity can [make a complaint to the Information Commissioner's Office \(ICO\)](#) or get advice from the ICO.

ICO contact details: Telephone: 0303 123 1113

This policy should be read alongside our:

Safeguarding and child protection policy

Safeguarding vulnerable adults policy

Childrens records policy

Photography and filming policy

Information technology policy

Confidentiality and client access to records policy

Privacy policy

Legal framework and references:

[Data protection](#)

[Data protection making a complaint](#)

[PACEY Record keeping guidelines](#)

[Information Commissioners Office – reporting a data breach](#)

This Policy was adopted by The Bumblebee Children's Charity and reviewed annually

Date 21.02.24

Name of signatory Lindsay Warne

Role of signatory Charity Administrator

Signed on behalf of the Trustees