Data Protection Policy

Contents

1. About this policy

1.1 Purpose

BucksVision is committed to respecting the privacy and confidentiality of all members, staff and volunteers. This policy sets out how we do so, and how we will comply with data protection legislation.

1.2 Risks and Implications

Failing to adhere to data protection legislation and good practice could put BucksVision's members at risk.

A breach of data protection, or failure to demonstrate good practice could put BucksVision at risk of significant financial penalties as well as reputational damage.

1.3 Scope

Who does this policy apply to?

This policy applies to anyone who accesses or uses BucksVision's data about members, staff or volunteers.

What does this policy apply to?

This policy applies to everything we do with information that identifies any living person. This includes how we collect, store, share, use and destroy such data.

1.4 Definitions

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated

means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority (ICO) and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

1.5 Roles and Responsibilities

The Trustee Board recognises its overall responsibility for ensuring that BucksVision complies with its legal obligations.

The Data Protection Officer is the Chief Executive, who has the following responsibilities:

- Briefing the Board on data protection responsibilities.
- Reviewing data protection and related policies.
- Advising staff on data protection issues.
- Ensuring that data protection induction and training takes place.
- Handling Subject Access Requests.
- Approving unusual or controversial disclosures of personal data.
- Ensuring contracts with data processors have appropriate data protection clauses.
- Electronic security.
- Approving data protection-related statements on publicity materials and letters.

Each member of staff and volunteer at BucksVision who handles personal data will comply with the organisation's operational procedures for handling personal data (including induction and training) to ensure that good data protection practice is established and followed.

All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

Significant breaches of this policy will be handled under BucksVision's disciplinary procedures.

2. Statements of the policy

2.1 Registered Data Controller

BucksVision makes decisions about how personal data is processed.

- The ICO registration details of BucksVision are reference number Z3413561 and Tier 1.

2.2 Transparency

BucksVision is committed to ensuring that data subjects are aware that their data is being processed and

- For what purpose it is being processed.
- What types of disclosure are likely.
- How to exercise their rights in relation to the data.

Data subjects will generally be informed in the following ways:

- Members (beneficiaries) - when they request (by any method) any of our services or referral to other service providers.
- Staff - in relevant policies (such as this one) and training.
- Volunteers - in their induction and through refresher training.

Standard statements will be provided to staff for use on forms where data is collected.

Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why, especially with respect to 'special categories' as stated previously under GDPR.

2.3 Direct Marketing

BucksVision will treat the following unsolicited direct communication with individuals as marketing:

- Seeking donations and other financial support.
- Promoting any of BucksVision's services.
- Promoting BucksVision's events.
- Promoting membership to supporters.
- Promoting sponsored events and other fundraising exercises.

- Marketing on behalf of any other external company or voluntary organisation.

Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and the data subject will be asked for their explicit consent to receive specific pieces of information, e.g., our quarterly newsletter. This consent will be recorded on our database with a note of the individual's preferred format (large print, electronic, etc).

BucksVision will only carry out telephone marketing where consent has been given in advance.

BucksVision will only use email communication if the individual has made it clear that this is their preferred format (e.g., for accessibility reasons) and they have given their explicit consent to receiving information by email.

2.4 Disclosure and Barring Checks (DBS)

As an organisation using the Disclosure and Barring Service (DBS) to help assess the suitability of applicants for positions of trust, BucksVision complies fully with the code of practice regarding the correct handling, use, storage, retention and disposal of certificates and certificate information, i.e., should usually be kept no longer than 6 months.

BucksVision also complies fully with its obligations under the General Data Protection Regulation (GDPR), Data Protection Act 2018 and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of certificate information.

- See Appendix 2 for further information.

2.5 Confidentiality

Because confidentiality applies to a much wider range of information than data protection, BucksVision has a separate Confidentiality Policy. This Data Protection Policy should be read in conjunction with BucksVision's Confidentiality Policy.

Staff, and volunteers are required to sign a short statement indicating that they have been made aware of their confidentiality responsibilities.

In order to provide some services, BucksVision may need to share an individual's personal data with other service providers (third parties). Verbal or written agreement will always be sought from the client before data is shared.

Where anyone within BucksVision feels that it would be appropriate to disclose information in a way contrary to the Confidentiality policy, or where an official disclosure request is received, this will only be done after discussions with the Operations Manager or Chief Executive.

All such disclosures will be documented.

2.6 Managing people's data securely

We take appropriate measures to prevent unauthorised processing of personal data, accidental loss or destruction of, or damage to, people's personal data. Information relating to our members, staff and volunteers is stored securely and only made accessible to authorised and trained staff and volunteers.

BucksVision has an Information Security policy. This sets out the standards we apply to how data is stored and accessed, along with our security standards, including the use of passwords and encryption.

BucksVision will ensure that business continuity measures are in place for our information assets. Business continuity measures will be agreed on a risk basis and are owned by BucksVision's Chief Executive.

2.6.1 Data Recording and Storage

BucksVision has a single database holding information about all members and volunteers. The data is backed up in secure cloud storage.

BucksVision will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- The database system is reviewed and re-designed, where necessary, to encourage and facilitate the entry of accurate data.
- Data on any individual will be held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets.
- Effective procedures are in place so that all relevant systems are updated when information about any individual changes.
- Staff and volunteers who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping.
- Data will be corrected if shown to be inaccurate.
- Should anyone request no contact, we will add them to our "do not contact" list.
- BucksVision stores archived paper records of members and volunteers securely in the office.

2.7 Data Subjects Rights

All individuals have legal rights relating to the information that we hold about them. These are set out in law, and can be found in Appendix 2. The Board of Trustees is responsible for the processes to deliver data subjects' rights.

- Requests for copies of personal data, or complaints about the way that BucksVision has processed people's personal data, must be forwarded to the Chief Executive.

2.8 Management of breaches, incidents and near misses

2.8.1 Any suspected incident or breach must be reported

An information security incident is any event that has the potential to affect the confidentiality, integrity or availability of our information, in any format, or IT systems in which this information is held. Any suspected breach or incident must be reported immediately by contacting the Data Protection Officer (i.e. Chief Executive).

If the incident clearly relates to the functioning of a BucksVision IT system, or an IT failure or concern, they should contact the IT helpdesk directly by phoning: 0333 344 5600.

2.8.2 The Data Protection Officer

The Data Protection Officer is responsible for investigating and recommending appropriate action in response to any suspected breaches of personal data security and will have oversight of action to be taken in response to loss or compromise of personal data, or systems and devices containing such information.

- The Data Protection Officer is responsible for liaising with the Information Commissioner's Office and reporting breaches in line with regulatory requirements to report any data breach that is likely to result in a risk to the rights and freedoms of data subjects within 72 hours of discovery.
- The Data Protection Officer in BucksVision is the Chief Executive.

2.8.3 Defining and reporting a 'personal data breach'

A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service".

A personal data breach may mean that someone other than the data controller gets unauthorised access to personal data. But a personal data breach can also occur if there is unauthorised access within an organisation, or if a data controller's own employee accidentally alters or deletes personal data.

- A breach of personal data will be notified to the Information Commissioner's Office following its guidance within 24 hours of discovery.

Other regulators, including the Charity Commission, will be notified of data breaches or security incidents as appropriate.

2.8.4 Learning from incidents, breaches and near misses

The Chief Executive provides updates as standing agenda item to the Board of Trustees on data protection including any incidents, breaches or near misses.

2.9 Staff Training and Acceptance of Responsibilities

All staff who have access to any kind of personal data are given copies of all relevant policies and procedures during their induction process, including this Data Protection Policy, Confidentiality Policy and the Information Security Policy. All staff will be expected to adhere to these policies and procedures.

Data Protection is included in the induction training for all volunteers.

BucksVision provides opportunities for staff to explore Data Protection issues through training, team meetings, and supervisions.

2.10 Third parties & processing data

In any case where a third party collects, stores or manages personal data on our behalf, BucksVision will ensure that there is a written agreement in place with that organisation, which must be reviewed by BucksVision's Legal team.

2.11 Data Protection and Safeguarding

Every member of staff has a role to play in BucksVision's Safeguarding approach. Any member of staff who has a safeguarding concern must record the information or allegation briefly, factually and accurately and then follow BucksVision's Safeguarding Policy

3. Policy Review

This policy is due for review every year or following any relevant and significant organisational or legislative change if earlier.

Reviewed by Chief Executive: 04/04/2023

Next review date: 04/04/2024

Version Control

Version	Date	Author	Changes
1.8	April 2023	Steve Naylor	Amended wording, added useful hyperlinks
1.7	June 2022	Alison Deuchars	Merged RNIB policy with BucksVision policy – added DBS paragraph
1.6	August 2019	Steve Naylor	Minor updates
1.5	November 2017	Steve Naylor	Clarified *Rights re: Automated Decision Making and Profiling*
1.4	October 2017	Steve Naylor	Updated to reflect GDPR
1.3	May 2017	Steve Naylor	Logo updated
1.2	April 2017	Steve Naylor	Updated to reflect RNIB Group changes
1.1	November 2015	Steve Naylor	Minor revisions made
1.0	November 2012	Alison Deuchars	Policy created

APPENDIX 1: The Rights of Data Subjects

- To make Subject Access Requests (SARs) regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- To not have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the GDPR.
- To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- To request the supervisory authority to assess whether any provision of the GDPR has been contravened.
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- To object to any automated profiling that is occurring without consent.

APPENDIX 2: Processing of DBS information

Storage and access
Certificate information should be kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

Handling
In accordance with section 124 of the Police Act 1997, certificate information is only passed to those who are authorised to receive it in the course of their duties. BucksVision must maintain a record of all those to whom certificates or certificate information has been revealed and it is a criminal offence to pass this information to anyone who is not entitled to receive it.

In addition, organisations that require retention of certificates in order to demonstrate 'safer recruitment' practice for the purpose of safeguarding audits may be legally entitled to retain the certificate. This practice will need to be compliant with the Data Protection Act, Human Rights Act, General Data Protection Regulation (GDPR), and incorporated within the individual organisation's policy on the correct handling and safekeeping of DBS certificate information.

Usage
Certificate information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Retention
Once a recruitment (or other relevant) decision has been made, we do not keep certificate information for any longer than is necessary, usually no longer than 6 months. This retention will allow for the consideration and resolution of any disputes or complaints, or be for the purpose of completing safeguarding audits.

Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will prevail.

Disposal
Once the retention period has elapsed, we will ensure that any DBS certificate information is immediately destroyed by secure means, for example by shredding, pulping or burning. While awaiting destruction, certificate information will not be kept in any insecure receptacle.

We will not keep any photocopy or other image of the certificate or any copy or representation of the contents of a certificate. However, notwithstanding the above, we may keep a record of the date of issue of a certificate, the name of the subject, the type of certificate requested, the position for which the certificate was requested, the unique reference number of the certificates and the details of the recruitment decision taken.