Data Protection, Information Security & Privacy Policy

FINAL V4.5

DEFINITIONS

Organisation	Means The Talk About Trust, a registered charity and it's trading subsidiary, the Pavilion in the Park (PiPs) Ltd
GDPR	Means the General Data Protection Regulation
Responsible Person	Means Chief Executive of the Talk About Trust
Register of Systems	Means a register of all systems or contexts in which personal data is processed by the charity as defined in the Data Audit
Basic Information	Means First Name, Last Name, Job Title, Email address, Business Name & Address.

Dated:	February 2025
Next Review Date:	February 2027

SECTION 1 – DATA PROTECTION

1.1 PURPOSE

Data protection and the preservation of your privacy is important to the organisation and we are committed to letting you know how we use your personal information and for making only responsible use of your data in line with GDPR.

In order to operate efficiently, the organisation collects information about people with whom the organisation works. These may include members of the public, schoolteachers, current, past and prospective employees, Board Members, volunteers, and partner organisations.

This document outlines the details of how the organisation deals with the data collected from the groups of people mentioned above.

1.2 DATA PROTECTION PRINCIPLES

The organisation is committed to processing data in accordance with its responsibilities under GDPR.

GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

1.3 GENERAL PROVISIONS

a) The policy applies to all personal data processed by the organisation
b) The Responsible Person will take responsibility for the organisation's ongoing compliance with this policy
c) This policy will be reviewed at least every 2 years
d) Where required, the organisation will register with the Information Commissioner's Office (ICO) as an organisation that processes personal data

1.4 LAWFUL, FAIR & TRANSPARENT PROCESSING

a) To ensure its processing of data is lawful, fair and transparent, the organisation will maintain a Register of Systems
b) The Register of Systems will be reviewed at least every 2 years
c) Individuals have the right to access their personal data and any such requests made to the organisation will be dealt with in a timely manner.

1.5 LAWFUL PURPOSES

a) All data processed by the organisation must be done on one of the following lawful bases: Consent, contract, legal obligation, vital interests, public task or legitimate interests (See ICO Guidance for more information)
a) The organisation will note the appropriate lawful basis in the Register of Systems
b) Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent will be retained by the organisation
c) Where communications are sent to individuals, the option for the individual to revoke their consent or object to processing will be clearly shown and systems will be in place to ensure such revocation is reflected accurately in the organisation's systems

1.6 DATA MINIMISATION

The organisation will ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

a) Newsletter Recipients - we will only collect basic information to allow us to keep them up-to-date, particularly with changes to our resources, general news via the newsletter or Pavilion updates as applicable
b) Trustee & Director Information – we will only collect the information required to govern the organisation in accordance with the Charity Commission Laws, Guidance for smaller charities and Company Law
c) Staff & Employee Information – we will only collect information needed under our safer recruitment policy, details to create our terms of employment, and other information necessary to carry out those terms of employment and information to satisfy payroll and HMRC requirements
d) Grants & Donations – we will only collect basic information regarding the funder plus details of any funding provided and related terms
e) Contracts – we will collect information necessary to enter into and meet the terms of any contracts
f) Paying Customers – initial card payment details will be provided to a third-party payment processor who specialize in the capture and processing of credit/debit card and PayPal transactions – your card information will not be held by us. We will also collect basic information to enable us to keep customers up to date, particularly with changes to our resources and general news via our newsletters.
g) Community Fundraising Supporters & other local contacts – we will only collect basic information to allow us to keep supporters up-to-date, particularly with local fundraising events and general news via our newsletters
h) Volunteers – we will only collect basic information needed under our volunteer policy

i) Community Room Bookings – we will only collect basic information associated with the booking
j) PiP Supper Club Bookings - we will only collect basic information associated with the booking
k) Media & Press - we will only collect basic information to allow us to keep them up-to-date, particularly with press releases

1.7 ACCURACY

a) The organisation will take all reasonable steps to ensure personal data is accurate.
b) If you change your email address or any other information, we hold is inaccurate or out of date, then please let us know by emailing info@talkabouttrust.org

1.8 ACCESS TO YOUR INFORMATION

a) The organisation will not sell or rent your information to third parties
b) The organisation will not share your information with third parties for marketing purposes
c) When using our online shop, the payment details will be used by our third-party payment processor who specialises in the secure online capture and processing of debit/credit card and PayPal transactions.
d) If you do not wish to receive communication from us about the vital work, we do to keep young people safe around alcohol then you can unsubscribe at any time by clicking 'Unsubscribe' at the bottom of our email communications or by sending an email to info@talkabouttrust.org
e) You have the right to ask for a copy of the information that the organisation holds. Any requests should be emailed to info@talkabouttrust.org.

1.9 ARCHIVING & REMOVAL

To ensure that personal data is kept for no longer than necessary, the organisation will adhere to the following retention periods, after which time the data will be deleted.

Group	Retention Period
1. Newsletter Recipients	We will renew our Privacy Notices every two years with the option to unsubscribe at any time
2. Trustee & Director Information - Recruitment of a new trustee/director - Current & Past Trustees/director	 Six months after recruitment process for unsuccessful candidates Three years after resignation
3. Staff Information - Recruitment of staff - Current & Past Staff	 Six months after recruitment process for unsuccessful candidates Three years after resignation (except HMRC data which will be seven years)
4. Grants & Donations - Current & Past Funders - Prospective Funders	 We will renew our Privacy Notices every two years with the option to unsubscribe at any time Within six months where support is not forthcoming
5. Contracts	We will renew our Privacy Notices every two years with the option to unsubscribe at any time

6. Community Fundraising Supporters & other local contacts	We will renew our Privacy Notices every two years with the option to unsubscribe at any time
7. Volunteers	Six months after recruitment process for unsuccessful candidates Three years after resignation
8. Community Room Bookings	We will renew our Privacy Notices every two years with the option to unsubscribe at any time
9. PiP Supper Club Bookings	We will renew our Privacy Notices every two years with the option to unsubscribe at any time
10. Media & Press	We will renew our Privacy Notices every two years with the option to unsubscribe at any time

1.10 BREACH

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to, personal data, the organisation will follow ICO Guidance to promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

SECTION 2 – INFORMATION SECURITY

2.1 GOVERNANCE

- The importance of information security should be reviewed at board level on a regular basis
- End-user instructions should be communicated to staff to outline expectations and responsibilities in upholding the security of the organisation
- Training should be developed and form part of the induction process for relevant staff

2.2 APPLICATIONS AND DEVICE OPERATING SYSTEMS

- Applications and operating systems must be updated promptly when vulnerabilities are rated as critical.
- User devices must have antivirus software installed with appropriate configurations such as scheduled scans and scanning files when these are accessed by users.
- The organisation uses Microsoft Office 365 and other standard applications and software – we do not have any bespoke applications.
- Personal data is stored securely using modern software that is kept up-to-date and is deleted when no longer required.

2.3 USER ACCESS

- Admin access for devices and/or applications should only be granted to a limited number of users.
- A user should only be granted admin access if it is needed to perform their job
- Complex passwords should be used for any admin accounts as it carries a greater risk if compromised
- Access to personal data shall be limited to personnel who need access
- All staff computers & laptops will have password protection in place to avoid unauthorised sharing of information.

2.4 PASSWORD MANAGEMENT

- Long, complex passwords are more secure than short, simple or repetitive passwords and staff are required to use the chosen Password Manager software to generate secure passwords
- Passwords should ideally be 10 characters long and contain a combination of uppercase and lowercase alpha and numeric characters and at least one special character (e.g., %, #,!).
- Any sharing of any passwords should be undertaken using appropriate encryption software (we recommend the use of Onetime Secret https://onetimesecret.com/)
- The use of shared user accounts should only be used where absolutely necessary and only with the prior approval of IT Support - passwords to these accounts must be shared securely and changed when staff with knowledge of the password leave the organisation.
- When end users receive passwords to user accounts the passwords must be shared securely.
- Where possible, IT systems should allow for end users to select their own password or change their password at first login.
- Default administrative passwords on devices should be changed.
- When an account compromise has occurred or is suspected, passwords on these end user accounts must be changed.

2.5 MULTI-FACTOR AUTHENTICATION

- Multi-Factor Authentication (MFA) should be used where possible when accessing sensitive data so that a potential attacker would need access to the 2nd authentication method (phone, email etc.) to gain access.

2.6 PORTABLE DEVICES

- Should be protected from unauthorised access when unattended – using a PIN or password or biometric methods.

2.7 BRING YOUR OWN DEVICE (BYOD)

- Anyone using their own device to access systems or data belonging to the organisation must follow the Bring Your Own Device Policy.

2.8 AWARENESS & TRAINING

All end users should have an understanding of:

- Password usage and management - Creation, frequency of changes, secure storage, multi-factor authentication (MFA).
- Policy - Implications of non-compliance.
- Emails - Attachments, links, phishing, spam, email list etiquette.
- Web usage - Appropriate usage (e.g., work-related internet browsing, file and content sharing via organisation approved platforms).
- Social engineering - Shoulder surfing, phishing, unusual activity, password resets
- Incident response - Roles, responsibilities and procedures (who to contact, what to do).
- Personal use - Use of systems at work and at home.
- Desktop - Screensavers, locking unattended screens.

Existing staff must receive appropriate refresher training on an annual basis.

2.9 REGULAR BACK-UPS

- All end users should schedule back-ups using One Drive.
- End Users should evidence that regular back-ups are in place on an annual basis.

2.10 REPORTING INCIDENTS

- All security incidents (either of a cyber nature or a physical nature) should be reported to the Finance & Governance Manager in the first instance.
- If necessary, the Finance & Governance Manager will seek professional technical support and report to the Information Commission Office if applicable

2.11 BUILDING SECURITY

- The last person to leave the Pavilion building is responsible for checking that all doors are secure and locked.
- The office should not be left with the external door unlocked if nobody is in the office during the day.

- The internal door to the office should be locked if people are using the community room out of hours.
- All cash should be securely locked in the safe or the cupboard in the office – the safe is insured for up to £4k and the cupboard in the office is insured for up to £500 - these limits should not be exceeded.
- All confidential papers should be kept in a locked cupboard.
- CCTV cameras will be in use at the Pavilion and scheduled to record from 5pm to 8am each day (which primarily covers when the cafe is closed).
- The CCTV cameras will be checked monthly to ensure they are working, and that the organisation can access the footage.
- A Fire Alarm system is in place at the Pavilion and is tested by the Cafe staff on a weekly basis and serviced annually by an approved engineer.

SECTION 3 – WEBSITE PRIVACY

The organisation has the following websites:
https://talkabouttrust.org
https://www.talkaboutalcohol.com
http://pipspoundbury.com and
Life Stuff (life-stuff.org)
The following website privacy policy applies to all of the above websites.

3.1 What is this Website Privacy Policy for?

This website privacy policy sets out how the organisation uses and protects any information that you give the organisation when you use our website.

The organisation is committed to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified when using our website, then you can be assured that it will only be used in accordance with this privacy policy.

The organisation may change this policy so users should check back from time to time to ensure they are happy with any changes. This policy is effective from 31st May 2023.

3.2 What we collect via our website

Where appropriate, we collect basic information to allow us to keep you up to date with the work of the organisation e.g. First Name, Last Name, Job Title, Email address, Business Name & Address. If you are using our online shop, then payment details will be provided to our third-party payment processor who specialises in the secure online capture and processing of debit/credit card transactions.

3.3 Security

We are committed to ensuring that your information is secure. In order to prevent unauthorized access or disclosure, we have put in place suitable physical, electronic and internal procedures to safeguard and secure the information we collect online.

3.4 How we use cookies

Our website uses cookies to better the users' experience while visiting the website. Where applicable our website uses a cookie control system allowing the user on their first visit to the website to allow or disallow the use of cookies on their computer / device. This complies with recent legislation requirements for websites to obtain explicit consent from users before leaving behind or reading files such as cookies on a user's computer / device.

Cookies are small files saved to the user's computers' hard drive that track, save and store information about the user's interactions and usage of the website. This allows the website, through its server, to provide the users with a tailored experience within our website.
Users are advised that if they wish to deny the use and saving of cookies from this website on to their computers hard drive, they should take necessary steps within their web browsers security settings to block all cookies from this website and its external serving vendors.

This website uses tracking software to monitor its visitors to better understand how they use it. This software is provided by Google Analytics which uses cookies to track visitor usage. The software will save a cookie to your computer's hard drive in order to track and monitor your engagement and usage of the website, but will not store, save or collect personal information. You can read Google's privacy policy here for further information [http://www.google.com/privacy.html].

Other cookies may be stored to your computer's hard drive by external vendors when this website uses referral programs, sponsored links or adverts. Such cookies are used for conversion and referral tracking and typically expire after 30 days, though some may take longer. No personal information is stored, saved or collected.

3.5 How to change your Cookies

First party cookies: Your web browser settings allow you to refuse any cookie or to alert you to when a cookie is being sent. They also allow you to control cookies stored on your hard drive.

Third party cookies: The above applies but as mentioned before the only third-party cookies we use are essential to complete certain tasks.

Please note that if you change your cookie settings, some of the features on our site may not work as well as we intend.

3.6 Links to other websites

Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should be aware that we do not have any control over that other website. Although our website only looks to include quality, safe and relevant external links, users are advised to adopt a policy of caution before clicking any external web links mentioned throughout this website and look at the privacy statement of the website in question.

The organisation cannot guarantee or verify the contents of any externally linked website despite their best efforts. Users should therefore note they click on external links at their own risk and this website, and its owners, cannot be held liable for any damages or implications caused by visiting any external links mentioned.

3.7 Social Media Platforms

Communication, engagement and actions taken through external social media platforms that this website and its owners participate on are custom to the terms and conditions as well as the privacy policies held with each social media platform respectively.

Users are advised to use social media platforms wisely and communicate / engage upon them with due care and caution with regard to their own privacy and personal details. This website nor its owners will ever ask for personal or sensitive information through social media platforms and encourage users wishing to discuss sensitive details to contact them through primary communication channels such as by telephone or email.

This website may use social sharing buttons, which help share web content directly from web pages to the social media platform in question. Users are advised before using such social sharing buttons that they do so at their own discretion and note that the social media platform may track and save your request to share a web page respectively through your social media platform account.

3.8 Shortened Links in Social Media

This website and its owners through their social media platform accounts may share web links to relevant web pages. By default, some social media platforms shorten lengthy urls.
Users are advised to take caution and good judgement before clicking any shortened urls published on social media platforms by this website and its owners. Despite the best efforts to ensure only genuine urls are published many social media platforms are prone to spam and hacking and therefore this website and its owners cannot be held liable for any damages or implications caused by visiting any shortened links.

3.9 Contact & Communication

Users contacting this website and/or its owners do so at their own discretion and provide any such personal details requested at their own risk. Your personal information is kept private and stored securely until a time it is no longer required or has no use, as detailed in GDPR. Every effort has been made to ensure a safe and secure form to email submission process but advise users using such form to email processes that they do so at their own risk.
This website and its owners use any information submitted to provide you with further information about the products / services they offer or to assist you in answering any questions or queries you may have submitted. This includes using your details to subscribe you to any email newsletter program the website operates but only if this was made clear to you and your express permission was granted when submitting any form to email process. Or whereby you the consumer have previously purchased from or enquired about purchasing from the company a product or service that the email newsletter relates to. This is by no means an entire list of your user rights in regard to receiving email marketing material. Your details are not passed on to any third parties.

3.10 Email Newsletter (applies to www.talkabouttrust.org and pipspoundbury.com only)

This website operates an email newsletter program, used to inform subscribers about products and services supplied by this website. Users can subscribe through an online automated process should they wish to do so but do so at their own discretion. Some subscriptions may be manually processed through prior written agreement with the user. Subscriptions are taken in compliance with GDPR. All personal details relating to subscriptions are held securely and in accordance with GDPR. No personal details are passed on to third parties nor shared with companies / people outside of the company that operates these websites.

Email marketing campaigns published by this website, or its owners may contain tracking facilities within the actual email. Subscriber activity is tracked and stored in a database for future analysis and evaluation. Such tracked activity may include; the opening of emails, forwarding of emails, the clicking of links within the email content, times, dates and frequency of activity [this is by no means a comprehensive list].
This information is used to refine future email campaigns and supply the user with more relevant content based around their activity. If you wish to disable tracking, then please unsubscribe from our mailing list.

3.11 Controlling your personal information

Under GDPR, you may request a copy of personal information held about you by this website's email newsletter program. If you would like a copy of the information held on you, please email info@talkabouttrust.org

In compliance with GDPR subscribers are given the opportunity to unsubscribe at any time through an automated system. This can be done by either unsubscribing at the bottom of your most recent email sent from us, by calling us on 01300 320 869 or by emailing info@talkabouttrust.org. Please note that unsubscribing from a particular newsletter will only remove you from that particular circulation list for that email address.

If you believe that any information, we hold is incorrect then please email us at info@talkabouttrust.org.

SECTION 4 – TALK ABOUT TRUST STORE VIA SUMUP - WEBSITE PRIVACY

The Talk About Trust (collectively “Merchant Store Name”, “we” and “us”, “data controller”) respect your privacy. We ensure that your privacy is protected when using our website or when placing online orders with us.

The Talk About Trust Trust provides you with goods and services and is the data controller of the personal data that you provide when you order goods.
The Data Protection Officer for The Talk About Trust can be contacted via contact form that can be found at the bottom of this page.

This Privacy Policy describes how your personal information is collected, used, and shared when you visit or make a purchase from talk-about-trust.sumupstore.com (the “Site”).

Personal data we collect

When you make a purchase or attempt to make a purchase through the Site, we collect certain information from you, including your name, billing address, shipping address, payment information (including credit card numbers), email address, and phone number. We refer to this information as “Order Information”.

When you visit the Site, we automatically collect certain information about your device, including information about your web browser, IP address, time zone, and some of the cookies that are installed on your device. Additionally, as you browse the Site, we collect information about the individual web pages or products that you view, what and which websites or search terms referred you to the Site, and information about how you interact with the Site. We refer to this automatically collected information as “Device Information”.

We collect Device Information using the following technologies:

- “Cookies” are data files that are placed on your device or computer and often include an anonymous unique identifier. For more information about cookies, and how to disable cookies, visit http://www.allaboutcookies.org.
- “Log files” track actions occurring on the Site, and collect data including your IP address, browser type, Internet service provider, referring/exit pages, and date/time stamps.
- “Web beacons”, “tags”, and “pixels” are electronic files used to record information about how you browse the Site.

How do we use your personal information?

We use the Order Information that we collect generally to fulfil any orders placed through and with the Site (including processing your payment information, arrangements for shipping, and providing you with invoices and/or order confirmations). Additionally, we use this Order Information to:
- Communicate with you;
- Screen orders for potential risk or fraud; and
- When in line with the preferences you have shared with us, provide you with information or advertising relating to our products or services.

We are processing your information in order to fulfil contracts we might have with you (for example if you make an order through the Site), or otherwise to pursue our legitimate business interests listed above.

We use the Device Information that we collect to help us screen for potential risk and fraud (in particular, your IP address), and more generally to improve and optimize our Site (for example, by generating analytics about how our customers browse and interact with the Site, and to assess the success of our marketing and advertising campaigns).

We also need to keep you up to date with any changes to our resources and other relevant updates as you have a professional interest in keeping young people safe around alcohol. We will use your personal information to send you our Teacher Newsletters, resource updates, details about our training events and other relevant mailings with the intention of keeping you updated on developments within the charity and on matters relating to alcohol education.

You can unsubscribe at any time by clicking the 'Unsubscribe' button at the bottom of any email or by contacting us at info@talkabouttrust.org.

Sharing your personal Information

We share your Personal Information with third parties to allow us to use your Personal Information, as described above. For example, we use SumUp to power our online store. We also use Google Analytics to help us understand how our customers use the Site -- you can read more about how Google uses your Personal Information here: https://www.google.com/intl/en/policies/privacy/. You can also opt-out of Google Analytics here: https://tools.google.com/dlpage/gaoptout.

We may share information with service providers under contract who help with parts of our business operations. Our contracts dictate that these service providers only use your information in connection with the services they perform for us and not for their own or any additional benefit.

Finally, we may also share your Personal Information to comply with applicable laws and regulations, to respond to a subpoena, search warrant and/or other lawful request for information we receive, or to otherwise protect our rights.

Transferring Information Internationally

We may transfer information collected about you to third parties acting on our behalf that may be located in countries outside of the European Economic Area ("EEA") or countries deemed by the European Commission to have satisfactory data protection. These other countries may not offer the same level of protection for the information collected about you, although we will at all times continue to collect, store and use your information in accordance with this Privacy Policy and the applicable data protection legislation. We will ensure we share data only with those organizations that satisfy an adequate level of data protection in line with applicable data protection legislation and that satisfactory contractual agreements are in place with any such parties.

Your rights

If GDPR is applicable to you, you have the right to access personal information we hold about you and to ask that your personal information be amended, updated, or deleted, you have the right to ask for the ceasing of processing of your data, object to profiling activities and solely automated processing, request that we restrict the processing of your personal data, and/or request that your data be transferred to a third party (data portability) under certain circumstances. If you would like to exercise this right, please contact us through the contact information below.

You have the right to withdraw your consent to the processing of your data at any time if the processing is based on your consent and can do so by contacting the DPO at the address provided.

If you would like to exercise any of your rights set out above, you can contact us using the contact form that can be found at the bottom of this page.

You also have a right to lodge a complaint with the relevant data protection authority.
The relevant authority for each country can be found on the European Commission website:
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080

Data retention

When you place an order through the Site, we will maintain your Order Information for as long as necessary to carry out our services to you or for as long as we are required by relevant laws. After this period, your personal data will be deleted.

Changes

We may update this privacy policy from time to time in order to reflect, for example, changes to our practices or for other operational, legal or regulatory reasons.

Contact us

For more information about our privacy practices, if you have questions, or if you would like to make a complaint, please contact us via contact form that can be found at the bottom of this page.

Our full Data Protection & Privacy policy is available to view at www.talkabouttrust.org.