Venn Primary Care Network Privacy Policy

Document Title: Venn PCN Privacy Policy
Version: *V1.0*
Effective Date: 3 June 2025
Review Due: 1 May 2026
Approval: Venn PCN

Introduction and Scope

Venn Primary Care Network ("Venn PCN") is committed to protecting the privacy and confidentiality of personal information. This Privacy Policy explains what personal data we collect and use in our PCN central functions, how we protect it, and your rights in relation to your data. It has been written in clear, plain English for accessibility and aligns with UK GDPR and the Data Protection Act 2018 ico.org.uk, as well as NHS England's privacy requirements in 2025.

This policy applies to Venn PCN's central operations and staff only – it does not cover personal data handled solely within individual member GP practices, which have their own privacy policies. (For example, each GP practice in the network will publish its own patient privacy notice. This Venn PCN policy covers any data processed by the PCN's central team for network-wide services or administration.

Who Are We?

Venn PCN is a collaborative group of GP practices in Hull working together to improve primary care services. The PCN's central team coordinates network-wide healthcare programs, extended access clinics, and administrative support for member practices. When Venn PCN's central team handles personal data (such as coordinating care across practices or running shared services), Venn PCN is a "data controller" for that information and must comply with data protection law. We have appointed a Data Protection Officer (DPO) and other key officers (see Contact Us section) to oversee data protection and confidentiality within Venn PCN.

What Information We Collect

Personal data is any information that can identify a living individual england.nhs.uk. The types of personal data Venn PCN may collect and use include:

- **Patient Data (Health Information):** If the PCN central team coordinates or provides clinical services (e.g. extended access appointments, clinical pharmacist reviews, social prescribing referrals), we will handle relevant patient records. This may include your name, contact details, NHS number, date of birth, health information (such as symptoms, diagnoses, medications, test results, referrals, care plans), and appointment history.

We only access medical information necessary to provide or arrange your care, in line with the Caldicott principles for patient confidentiality (using the minimum necessary information and on a need-to-know basis) gov.ukgov.uk.

- **Staff and Contractor Data:**
  For people employed by or working with the PCN central team (e.g. clinical pharmacists, social prescribers, administrative staff), we hold personal details needed for employment or engagement. This includes contact information, qualifications, HR records, payroll details, and any necessary occupational health information.
- **Member Practice Contacts:**
  We may hold business contact details of key staff at member GP practices or partner organisations for communication and coordination purposes (e.g. names, work emails/phones of practice managers or clinicians involved in PCN services).
- **Service Users and Public Queries:**
  If you contact the PCN's central office (for example, with an inquiry or to attend a PCN-organised event or programme), we may collect your name and contact information and any details you provide so we can respond or provide the service.

We aim to collect data directly from you or from your registered GP practice (for patient information) whenever possible. In some cases, we might receive information from other NHS organisations – for example, hospital or community providers may share data with the PCN when we jointly coordinate your care. We ensure any data collected is relevant and limited to what is necessary for the intended purpose (data minimisation principle).

How We Use Your Information

Venn PCN uses personal data only for specific, legitimate purposes in support of healthcare and network administration. Under no circumstances do we sell personal data or use it for purposes incompatible with those outlined here. The main purposes for which we use data are:

- **Direct Care and Clinical Services:**
  We use patient information to provide or support healthcare services that the PCN central team delivers. For example, if you attend an extended access evening/weekend clinic run by the PCN, the clinician will access your medical history to treat you, and will update your record with details of the consultation. This ensures you receive safe, informed care and that your GP is kept updated. We only use the confidential health information required to care for you, and all staff are bound by the NHS duty of confidentiality.

- **Care Coordination:**
  The PCN may use relevant patient data to coordinate services across member practices and other providers. For instance, our team might review practice registers (e.g. of patients with certain conditions) to plan network-wide health programmes or outreach (such as vaccination clinics or health coaching programs). When doing so, we work closely with your GP practice and follow strict governance so that any data used is properly authorised and kept secure.

- **Referral and Signposting Services:**
  If the PCN's social prescribing link workers or other staff help refer you to community services or clinics, they will use your details to make those referrals with your consent/knowledge. Similarly, if we arrange specialist clinics or multi-disciplinary team meetings, we use relevant information to refer or discuss your case with appropriate professionals (always ensuring only those involved in your care have access).

- **Service Evaluation and Planning:**
  We may aggregate and analyse data to review the quality and outcomes of PCN services. For example, we might track how many patients attended a new clinic or general trends in health indicators to improve services. Wherever possible, we use anonymised or aggregated data for planning (data that does not identify individuals). If identifiable data is needed for an audit or review, we either get patient consent or have an approval under NHS confidentiality rules.

- **PCN Administration and Finance:**
  We use personal data of staff for employment administration (payroll, performance, etc.), and data of patients or service usage for commissioning and funding claims. For example, we might need to report pseudonymised service usage data to the NHS for funding purposes. Any such reporting will either not include personal identifiers, or if identifiers are needed (e.g. NHS number for validation), this is done under secure, authorised processes.

- **Communicating with You:**
  If you reach out to the PCN central team with a query or request, we will use your contact information to communicate and resolve your inquiry. We may also, with your permission or as allowed, send you information about services such as appointment reminders or program invitations.

  For instance, if the PCN organises a health education event, we might invite relevant patients. You can always opt out of non-essential communications. (Note: Routine communications about your care, such as appointment reminders, are considered part of healthcare and use your contact details accordingly. We ensure these use secure channels – e.g., using NHSmail for emails or official text messaging systems – see How We Protect Your Data below.)

We do not use your data for marketing or advertising purposes unrelated to your care. We also do not use automated decision-making or profiling on your data without human involvement. If we ever intend to use data for a new purpose not covered by this policy, we will update this notice and/or seek consent as appropriate.

Lawful Basis for Processing

We must have a valid lawful basis under the UK GDPR for each use of personal data, and for "special category" data like health information we need an additional condition. Venn PCN relies on the following legal bases:

- **Provision of Healthcare (Public Task):**
  Most patient data processing by the PCN central team is for direct care or healthcare management. The lawful basis under Article 6 UK GDPR is typically **"**exercise of official authority / task in the public interest" – because GP practices (and by extension the PCN as part of NHS primary care) provide medical services as a public task.

  The additional condition under Article 9 (for health data) is "medical diagnosis or provision of health care or treatment" (UK GDPR Art.9(2)(h) and Schedule 1 of DPA 2018) or "public interest in public health" as applicable. This means we can use health information to care for you without explicit consent, as there is a legal duty and public interest in doing so, and we apply strict confidentiality and security.

- **Legal Obligations:**
  In some cases we process data because we have a legal obligation. For example, we must report certain information for public health or safety (like communicable disease notifications or safeguarding concerns). Also, we have to retain records for set periods by law (see Retention section). Article 6(1)(c) "compliance with a legal obligation" covers these cases. (Where health data is involved, additional conditions could include those laid out in law for public health or safeguarding functions.)

- **Contract (Staff Data):**
  For our employees and contractors, we process personal data as necessary to fulfil our employment contracts and management responsibilities. For instance, processing salary and tax information is based on the employment contract and legal obligations to HMRC. Health data about staff (like sick notes or occupational health reports) is processed under the employment law obligations and for assessment of working capacity (DPA 2018 Schedule 1 conditions).

- **Consent:**
  Generally, we do not rely on consent for core PCN healthcare services, since we have other bases as above. However, we will seek consent in specific situations where needed – for instance, if we wish to use your photo or testimonial on a PCN newsletter, or if we invite you to an optional research project or trial. If consent is used, it will be informed and voluntary,

and you can withdraw it at any time. Withdrawing consent will not affect your normal care.

- **Vital Interests:**
  In a rare emergency where someone's life is at stake and they cannot give information or consent, we may use or share personal data as necessary to protect their vital interests. This is only for urgent situations (e.g. providing details to ambulance staff if a patient collapses at a PCN site).
- **Public Interest / Official Authority (non-care):**
  Sometimes the PCN may process data for broader health system planning or audits mandated by NHS England or the local Integrated Care Board. When doing so, we ensure an appropriate basis applies, such as tasks carried out in the public interest (e.g. ensuring quality of care, fraud prevention audits, or service planning). Wherever possible, identifiable data is minimised or pseudonymised for these purposes.

We will always ensure a valid basis applies before processing personal data. If you have questions about the legal basis for a particular use of your data, please contact our DPO.

How We Share Information

Your data is kept confidential within the PCN and shared only when genuinely needed. We sometimes need to share information with others to support your care or manage services, but we do so under strict conditions:

- **Member GP Practices:**
  Your registered GP practice and the PCN central team share data as needed for your care. For example, if a PCN pharmacist reviews your medications, they will update your GP record. The PCN may also receive limited data from practices (like patient lists) to arrange services. This sharing is inherent in how PCN and practices work together, and it is done under data sharing agreements or contracts that ensure all parties protect the data.
- **Other NHS Providers:**
  We might share relevant information with other healthcare providers involved in your treatment, such as hospitals, community nursing, mental health services, or out-of-hours clinics. For instance, if you attend a PCN clinic and need a hospital follow-up, we will send a referral with necessary details. Or if a community service (like a physiotherapist or social prescriber) is helping with your care, we may share information with them. In all cases, we only share what is necessary and ensure the recipient is authorised to have it (usually they are NHS or social care professionals subject to confidentiality).
- **Commissioners and NHS Bodies:**
  The PCN may share data with NHS commissioning organisations (like our local Integrated Care Board or NHS England) for planning, payment and

performance monitoring. Often this will be aggregated or de-identified data (not linked to named individuals). If any identifiable data is required (for example, validating that a service was provided to a patient), this is done via secure NHS systems and under a legal mandate or contract.

- **Service Providers (Data Processors):**
  Venn PCN uses certain third-party service providers to help deliver our services – for example, we might use an electronic records system, an appointment booking software, or secure data storage/IT support services. These providers may process personal data on our behalf. We always have contracts in place with such processors to ensure they meet NHS data protection standards and only use the data under our instructions. We do *not* allow them to use your data for any other purposes.

- **Lawful Disclosures:**
  In some situations, we are legally required to share information. For example, we must report notifiable diseases to Public Health authorities, or provide information to regulators or a court if ordered. We may also share information with authorities if required for safeguarding vulnerable individuals or preventing serious harm (under proper legal basis and usually with advice from our safeguarding lead or Caldicott Guardian). If a request from police or another third party for personal information is received, we will only disclose data if the request meets legal criteria (such as a court order or under an exemption in data protection law) – otherwise, we will politely refuse or refer them to the patient's GP.

- **National Programs and Registries:**
  There are some national NHS programs where data is collected for the public good (for instance, the National Disease Registries or NHS Digital data collections). If the PCN is involved in such programs, we will ensure patients are informed (usually via national NHS communications and our own notices) and that any required opt-outs are respected (see National Data Opt-Out below).

- **With Your Consent:**
  Apart from the above, if any other sharing is proposed, we will explain the reason and obtain your consent when required. For example, if you want your family or caregiver to be kept informed about your care, we would record and respect your consent to share with them.

Whenever we share data, we do so using secure methods. This could include secure NHS email (nhs.net accounts with encryption), approved healthcare IT systems, or hand-delivery of paper records if absolutely necessary. We do not transfer your personal data outside of the UK unless it is via an NHS-approved system or provider that meets UK data protection standards (for instance, some NHS IT systems are cloud-based with servers in the EEA under adequacy agreements – any such transfer would be compliant with UK GDPR transfer requirements). If you have questions about a particular sharing or transfer, please contact us.

How We Protect Your Data
Venn PCN takes information security and confidentiality very seriously. We have implemented a range of technical and organisational measures to protect personal data from unauthorized access, loss, or damageengland.nhs.uk. These include:

- **Staff Training and Confidentiality:**
  All PCN staff, clinicians, and volunteers must sign confidentiality agreements and complete annual data protection training (the NHS Data Security Awareness training) england.nhs.uk. We ensure everyone is aware of their personal responsibilities to keep data secure and private gov.uk. Only authorised staff who need information for their role can access it (**role-**based access control). Our team follows the eight Caldicott Principles for handling patient-identifiable data, ensuring justified purposes, minimum necessary use, and strict need-to-know access at all times gov.ukgov.uk.

- **Access Controls:**
  Electronic health records and systems used by the PCN are password-protected and accessible only via authenticated NHS smartcards or secure logins. We enforce strong password policies and use two-factor authentication where available. Each user's access rights are limited to what they need (for example, a social prescriber can only see relevant referral information, not entire medical histories, unless required for care).

- **Secure Networks and Devices:**
  We use NHS-approved secure networks for data (such as the NHS N3/HSCN network and secure NHSmail for emails). PCN laptops and devices are encrypted to NHS standards, and portable media (USB drives, etc.) are avoided or also encrypted. We have policies in place for remote working – staff working from home or off-site must still ensure confidentiality (for example, not sharing screens where others can see, using VPN and secure connections, keeping paperwork safe) england.nhs.uk. We prohibit sending patient-identifiable information over insecure channels (no use of personal email accounts or unsecured messaging for work purposes).

- **Physical Security:**
  Any physical records (paper documents) are kept in locked cabinets in secure PCN office premises. Our offices have controlled access. Staff are instructed to clear desks of sensitive papers and not leave documents or laptops unattended. When transporting records (if ever necessary), we use sealed containers and documented handover.

- **Data Minimisation and Pseudonymisation:**
  We try to store or use identifiable data only when needed. For analysis or reporting, we remove identifiers or use codes where possible (pseudonymised data) digital.nhs.uk. This means even if data were accessed, it might not directly identify individuals without the key.

- **Anti-Malware and IT Security:** All our computers and systems have up-to-date antivirus and malware protection. Security patches are applied regularly. We follow NHS Digital cybersecurity guidance and work with our

IT providers to guard against threats. There are firewalls and intrusion detection on our networks.

- **Monitoring and Audit Trails:**
  Systems maintain audit logs of who accessed records and when. We perform periodic audits to ensure staff access is appropriate. Any unusual access or behaviour triggers an alert for investigation.
- **Incident Response:**
  We have an internal procedure for responding to any data breaches or security incidents (see the Data Breach Procedure summary below). Staff must immediately report any lost data, security lapse, or suspicious activity. We will act swiftly, containing and investigating the issue. If a significant data breach occurs, we will inform affected individuals and report to regulators (ICO, NHS) as required england.nhs.uk.
- **Data Protection by Design:**
  When introducing any new system or process that involves personal data, we carry out a Data Protection Impact Assessment (DPIA) to identify and mitigate privacy risks. This helps embed strong privacy and security controls from the start of any project, in line with NHS best practices.

By following the National Data Guardian's 10 Security Standards and NHS Digital guidance, and completing the annual Data Security & Protection Toolkit (DSPT) self-assessment england.nhs.uk, Venn PCN continually reviews and improves our data protection measures. In summary, we do everything reasonably possible to prevent unauthorised use or disclosure of your data. If you have specific questions about our security measures, please reach out to our DPO.

How Long We Keep Information (Retention)
We do not keep personal data longer than necessary for the purpose it was collected. Retention periods for NHS records are determined by the NHS Records Management Code of Practice 2021, which provides guidance on how long different types of records should be kept digital.nhs.uk. Venn PCN adheres to these standards:

- **Patient Health Records:**
  Clinical information recorded in your GP record as part of PCN services becomes part of your lifelong medical record. GP records are generally kept for at least your lifetime and normally 10 years after death (as per NHS policy), since continuity of care is important. If the PCN holds any separate clinical logs or data for services provided, we either incorporate them into the GP record or retain them for the same duration as GP records, to ensure consistency.
- **Service-Specific Records:**
  If the PCN maintains records for specific programs (e.g. a diabetes education program attendance list), we will keep those records only as long as needed for that purpose and any reporting requirements. Often, we will

anonymise or delete personal identifiers once the program and any follow-up is complete, unless it needs to be linked to your health record.

- **Staff Records:**
  HR/personnel files are typically kept during employment and then for a period after an employee leaves (commonly 6 years after leaving, in line with employment law limitation periods). Some records (like pension or health and safety records) may be kept longer if required by law.
- **Administrative Records:**
  Emails, meeting minutes, and project documents that contain personal data are periodically reviewed and deleted when no longer needed. We follow NHS guidelines for administrative record retention (usually between 2-7 years depending on the record type and its purpose).
- **CCTV or Call Recordings:**
  (If applicable – for example, if the PCN office uses CCTV or records phone calls for training) such data is typically retained for a short period (e.g. 30 days for CCTV unless needed for an investigation). We will signpost any such usage on signage or when you call.

When a retention period is reached, we ensure data is securely disposed of or archived. Paper records are shredded via a confidential waste service (meeting standards for destroying sensitive documents) digital.nhs.uk. Electronic data is securely deleted or overwritten – we follow National Cyber Security Centre guidance for secure deletion digital.nhs.uk. Backup copies are also deleted in due course. If we archive data (store it beyond active use, for historical or legal reasons), we still protect it and restrict access.

In summary, we keep your information only for as long as necessary and then erase or anonymise it safely. For more details, you can request a copy of our Records Management Policy or schedule (which aligns with the NHS Records Management Code).

Your Rights Over Your Data

Under data protection law, you have several important rights regarding your personal data. Venn PCN is committed to upholding these rights. They include:

- **Right to Be Informed:**
  You have the right to be informed about how and why your data is used. This Privacy Policy, along with other notices we provide, is intended to give clear information. If anything is unclear, you can ask us questions.
- **Right of Access:**
  You can request a copy of the personal data we hold about you, which is known as a Subject Access Request (SAR). For example, patients can request to see their health records held by the PCN or GP practice. We will confirm whether we process your data and provide a copy typically within one month (free of charge)england.nhs.uk.

We may ask for proof of identity and clarification on the data you need, especially if the request is complex. (Note: Most patient data we handle is also in your GP record, which you can access via your practice or NHS app. But you have the right to request from us directly as well.)

- **Right to Rectification:**
  If you believe data we hold about you is inaccurate or incomplete, you can ask us to correct it. We will rectify any factual errors or add notes to clarify incomplete information without undue delay. For example, if your contact address changes or you spot an error in a record, let us know and we will update it.

- **Right to Erasure:**
  In certain circumstances, you may request that we delete your personal data (this is sometimes called “the right to be forgotten”). However, this right is not absolute and does not usually apply to medical records or where we have a legal obligation to keep data. For instance, we generally cannot erase health records that are needed for continued care or required by NHS retention rules. We will consider any request and explain what can be done. If we cannot delete (e.g., your medical records), we may be able to restrict processing (see below).

- **Right to Restrict Processing:**
  You can ask us to restrict or pause the use of your data in certain situations – for example, if you contest its accuracy or have objected to processing (pending resolution). During restriction, we can store the data but not use it. If applicable, we will mark the record as restricted and inform you of any change.

- **Right to Object:**
  You have the right to object to certain types of processing. For example, you can object to your data being used for purposes beyond your direct care, such as research or planning, unless there is an overriding legal reason. If you object, we will consider your request and whether we must comply or have compelling grounds to continue. You also have an absolute right to object to any direct marketing, but Venn PCN does not perform marketing with patient data.

- **Right to Data Portability:**
  This applies mostly to data you provided us yourself, which we process by automated means on the basis of consent or contract. It allows you to obtain that data in a commonly used electronic format and reuse it elsewhere. This is seldom relevant in healthcare settings (as we don’t typically process data on consent for services), but if applicable we will provide the data in CSV or similar format.

- **Rights related to Automated Decision-Making:**
  Venn PCN does not make any purely automated decisions that have legal or significant effects on individuals (such as algorithm-only decisions without human review). If that ever changes, we will inform you and ensure your rights to human review of decisions and to express your point of view are protected.

To exercise any of these rights, you can contact us (see Contact Us below). We will respond as quickly as possible, usually within one month. There is no fee for making a request, unless it's unfounded or excessive (in which case we may charge a reasonable fee or refuse, but we will explain why). For certain requests, we might need to verify your identity to protect your privacy (for example, making sure we only release data to the correct person).

Please note that your rights may be limited by other obligations – for instance, we cannot release information that includes another person's data without their consent, and we might need to redact third-party information in records we provide to you. Also, if you are requesting on someone else's behalf, we will need proof of your authority (such as a power of attorney or parental rights if for a child).

Overall, we support your rights fully and aim to facilitate them. If you have any concerns about your rights or our handling of a request, do let our DPO know. You also have the right to complain to the ICO if you believe we are not complying with the law (see Complaints below).

National Data Opt-Out
Patients in England can choose if their confidential patient information is used beyond their own individual care – for example, for research or planning of health services. This choice is managed through the National Data Opt-Out program. Venn PCN respects and complies with the national data opt-out.

- **What is the National Data Opt-Out?**
  It is a service that allows you to opt out of your identifiable health data being used for purposes other than your direct care. This was introduced on 25 May 2018 (replacing older "Type 2" opt-outs) bytespcn.nhs.uk. If you opt out, NHS organizations should not share your confidential data for research or planning unless there is a legal requirement (for example, a public health emergency) or you consent separately.

- **How We Comply:**
  Before Venn PCN participates in any project that uses patient data for secondary purposes (like research studies, or sending data to an NHS registry that is not for your direct care), we will apply the national opt-out settings. Practically, this means if you have an opt-out registered, we will exclude your data from the extract or use, unless there is an overriding exemption. We have systems to check opt-out flags, usually via NHS Digital's service.

- **Your Choices:**
  Registering an opt-out is done centrally (you can do it online at www.nhs.uk/your-nhs-data-matters or via a phone service or form). You do not need to inform each GP or PCN – once set, it applies across the NHS. If you have previously told your GP about a Type 1 opt-out (which is a separate choice to not share your GP record outside for anything other than direct care), that is maintained at your practice and the PCN honours those as well when accessing or using data.
- **Impact:**
  Choosing the opt-out will not affect your individual care. You will still be included in screenings, receive care, etc. It only affects uses of data for planning/research. We will ensure that even if you opt out, you still benefit from all direct care services we offer.
- **Changing Your Mind:**
  You can opt out or back in at any time via the NHS website mentioned above. Our staff can provide information leaflets or guidance if you need help with the process.

For more information on the national data opt-out policy, you can visit nhs.uk/your-nhs-data-matters or contact the PCN for a leaflet.

(Note: The National Data Opt-Out is a separate choice from "Type 1 opt-out" which relates to not sharing your GP record for purposes beyond care. Type 1 opt-outs are managed at your GP practice; if you have one, it means your full record won't be extracted for planning/research by NHS Digital. Both Type 1 and the National opt-out will be respected by the PCN in any data uses.)

Contact Us (Queries, DPO, and Exercising Rights)
If you have any questions about this Privacy Policy or about how Venn PCN uses your information, please get in touch. You can also contact us to exercise your rights (access, correction, etc.) or to discuss any concern.

- **Venn PCN Contact:**
  Joan Cummings
- **joan.**cummings1@nhs.net
  Please mark any correspondence regarding data protection as "FAO Data Protection Officer" for proper handling.
- **Data Protection Officer (DPO):**
  Barry Jackson
- **barry.**jackson@nhs.net
  The DPO is a specialist advisor independent of our operational team who oversees data protection compliance. You may contact the DPO directly for

any privacy concerns or if you feel your questions have not been answered by the PCN team.

- **Caldicott Guardian:**
  Dr Amy Oehring

- *Amy.oehring@nhs.net*
  This is a senior clinician responsible for protecting patient confidentiality and enabling appropriate information sharing. They can advise on ethical and confidentiality questions. (Usually, you would contact them via the PCN office or through the DPO for any such queries.)

- **Senior Information Risk Owner (SIRO):**
  Joan Cummings
- **joan.**cummings1@nhs.net

  This is a senior person responsible for managing information risks in the PCN. They ensure we have the right policies and that risks (like data breaches) are properly managed.

When contacting us, please include details of your request or question, and your contact information. For Subject Access or other rights requests, if you can specify which information or processing you are referring to, it helps us respond faster. We may need to verify your identity especially if you're requesting personal data.

Complaints and Further Advice
We hope we can address any questions or issues you have. However, if you are unhappy with how we have handled your personal data or your requests, you have the right to complain to the Information Commissioner's Office (ICO). The ICO is the UK's independent regulator for data protection.

- **ICO Website:**
  ico.org.uk/make-a-complaint or ico.org.uk/global/contact-us/
- **ICO Helpline:**
  0303 123 1113
- **ICO Address:**
  Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

We would appreciate the chance to deal with your concerns before you approach the ICO, so please do contact our DPO or PCN management first if possible. We are committed to resolving any issues in a fair and transparent way.

Policy Review

This Privacy Policy will be reviewed at least annually and updated to reflect any changes in how Venn PCN processes personal data or to remain compliant with changes in the law or NHS requirements. The version and date at the top indicate the last update. We will communicate any significant changes via our website or direct notices. Please ensure you have the latest copy. Your continued interaction with our services after updates will indicate acceptance of the revised policy.