Mental Health Hub

CORDS
Child Outcomes
Record Data System

Protecting and Securing your Data

Data Protection Officer: DS Compliance

October 2023

Data Protection at Mental Health Hub

Geographical area: United Kingdom (UK)

Policy created: September 2022 (Marcus Dyke)
Last updated: October 2023 (Marcus Dyke)
Review date: December 2024

In this document, you will find the following policies and documents:

Mental Health Hub Privacy Policy

Mental Health Hub Cookies Policy

CORDS Security Whitepaper

CORDS Privacy Policy

CORDS Data Sharing Agreement

If you are unable to find what you are looking for, please contact us.

Review

At any time and at our discretion, we may vary this document (and subsequently our policies) by publishing the amended document on our website.

We will endeavour to provide you with a notice of change of this document if any amendments occur, but as part of your due diligence, we recommend you check www.mentalhealthhub.com regularly to ensure you are aware of our current policies.

If you do not agree with the amendments, please close your account and discontinue the use of our services and site, otherwise, you will be deemed to have consented expressly to any updates.

Contact Details

To exercise your Privacy Rights, please contact our Data Protection Officer who is responsible for our data protection and will be the most appropriate person to support you.

DS Compliance
Quadrant House
4 Thomas More Square
London
E1W 1YW
info@ds-compliance.com
020 7175 3472

Mental Health Hub
145 London Road
Kingston upon Thames
KT2 6SR
contact@mentalhealthhub.com
020 4524 1008

If you have any concerns about our handling of your Personal Information, we would like the opportunity to investigate it for you and put things right, so please get in touch with our Data Protection Officer to let us know what went wrong.

If you are not happy with our response, you have the right to complain to the Information Commissioner's Office: www.ico.org.uk/make-a-complaint

Information Commissioner's Office (ICO)
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113
Website: www.ico.org.uk

Overview

We take our responsibilities for privacy and your data security extremely seriously.

The purpose of this Privacy Policy is to provide you with a clear explanation of when, why and how we collect and use your personal and health information, as well as an explanation of your statutory rights.

We strongly urge you to read this policy and make sure you fully understand it, before you access or use any of our services.

Child Outcomes Record Data System (**CORDS**) is a trading name of, and a system wholly owned and operated by, The Mental Health Hub Ltd (**Mental Health Hub**).

The Mental Health Hub Ltd (Company Number: **11406287**) is a limited company, registered in England and Wales.

Mental Health Hub is registered with the Information Commissioners Office (ICO) (Registration Number: **ZB423206**)

CORDS and Mental Health Hub will also be referred to as **we**, **us** or **our** throughout.

We are committed to protecting the privacy of personal information provided to us and to complying with the Data Protection Act 2018 (the Data Protection Act), the UK GDPR and (where applicable) the EU GDPR.

Our Privacy Policy outlines how we collect, use and disclose your information when you access or use our website located at **cords.app**, **mentalhealthhub.com, members.mentalhealthhub.com** or our other websites (the Site, Sites), our mobile applications (the App, Apps) and other online or offline services, in each case that we own and/or operate and that link to this Privacy Policy (collectively, the Services) and when you otherwise interact with us, and the rights and choices available to our visitors and users regarding such information.

By using our Services, you agree that we may treat your information in the ways we describe in this Privacy Policy. If you do not agree with any terms of our Privacy Policy, you may not use our Services.

Our Privacy policy and notice provide transparency to our users as to how their data is collected and used and serve as a privacy notice as required by legislation.

We treat security as a first-class concern at Mental Health Hub.

All data (customer records, file attachments, images) that are in transit and at rest are encrypted by default using industry-standard AES 256-bit encryption.

Personally identifiable information is treated with additional encryption to protect this information from our third-party service providers.

Your data is backed up hourly, weekly, and monthly to ensure we can recover your data in the event of server or database failures.

Our team are trained to handle your customer data with utmost care. Access to production environments is restricted to only senior team members with the "least privilege" principle.

Monitoring and audit logs are enabled in all critical points (infrastructure and databases). This enables us to take appropriate actions to prevent, or mitigate, any potential security issues.

We adhere to leading health information standards in accordance with GDPR and the UK Data Protection Act.

At CORDS, we believe the power of technology can help mental health providers innovate and elevate the efficiency and quality of their care delivery. To deliver on our purpose to help millions of people access proactive, personalised, outcome-driven mental health care we use modern digital touchpoints to capture and organise relevant information to support our customers.

The digitisation of traditional data collection and engagement requires high-security standards in all areas to protect and secure all user data.

In our Security Whitepaper, we outlined all the appropriate steps and practices we implemented to safeguard privacy and user data.

Mental Health Hub Websites Privacy Policy

Introduction

This policy describes how we capture and use personal data that we collect about visitors to our websites.

Please read this information carefully to understand our views and practices regarding your personal data and how we will treat it.

Mental Health Hub acts as a data controller for all personal data, which the Mental Health Hub customers and site visitors input.

For the personal data which the account holder's survey respondents fill out on any of the surveys commissioned by the customer, Mental Health Hub acts as a data processor, processing only in accordance with the customer's instructions. The customer in these circumstances is the data controller.

This policy has been structured in two parts as follows:

- **Section 1** - Privacy of Customers
- **Section 2** - Privacy of all site visitors

Definitions

- A "**customer**" or "**user**" is anyone who has been authorised to have a CORDS account.
- A "**respondent**" is anyone who completes an assessment, survey or interaction on CORDS.
  A "**site visitor**" is anyone who visits the www.mentalhealthhub.com website.

Privacy of Customers

The data we collect from you.

We collect the following data from you:

- Account and Billing Information: this is the information you put on when opening an account including your name, school, email address etc
- Account Settings and Preferences
- Address Book: including any email addresses and names you specify
- Any other information you share with us including support tickets, emails, queries and case studies
- The legal basis for us collecting the above data is that it is necessary for us to provide you with the services under your contract(s)

Billing Information

We request information from a customer by capturing this on the order form. A customer must provide contact information (for example, name, email, and address) and associated billing details. This information is used for billing purposes and to fulfil your order. If we need to contact you to discuss an order, the information is used to contact you.

What do we do with the information we collect?

We use the information we collect to provide our services to you. This includes:

- Providing you with customer support and help with our services when you contact us
- Contacting you about your account, billing information, changes to our terms, changes to other policies, and any other issues regarding our services
- For troubleshooting and testing of our services to ensure that it is secure, reliable and of a high standard
- Maintain and improve our services
- To enforce our Software License Agreement to ensure you are not carrying out any prohibited activities
- To prohibit illegal activity using our services
- To respond to legal requests, court orders or lawful requests from government agencies
- For providing our services to you as per your request

Marketing and promotional emails

Where you have consented, we will contact you regarding promotional activities and marketing in order to inform you about offers and helpful tips about our service, you have a right to withdraw that consent at any time by following the simple instructions on the email or contacting us to advise that you no longer wish to receive promotional emails. Please also see your rights below.

Sharing and disclosure of your data

We use processors to store our data safely and securely. All assessment and survey data is stored in the EEA and all our processors have robust security features to ensure that they have the appropriate technical and organisational measures to keep personal data secure.

Your data to third countries

Some of our sub-processors may process data outside of the EEA. We do not transfer your data outside of the EEA. Any data (unless you consent otherwise) is stored in the EEA at all times. You may withdraw that consent at any time by contacting us.

Backup policy

All data you hold with us is backed up in separate physical premises with technical and organisational measures equal to the places where the original data is held. This is to ensure that your data is not lost or destroyed should the original be destroyed without your instructions.

Rights to your data

If you are a customer, you have the following rights to your data:

Right to access

You have the right to access the data we hold about you. If you would like all of the information we hold about you, please contact us.

We will process your request without undue delay and at the latest within 1 month, unless your request is complex or numerous in which case, we may take up to 3 months, but we will inform you within 1 month if this is the case.

Right to rectify

You can also rectify or update any information on your account. If you wish to do so, please contact us with the amended information.

Right to erase

When you log on to your account, you may also erase any data on your account with the exception of data that is required for you to keep your account open (such as your email address, name etc). You also have the right to erase any other data which we hold about you, including raising any questions or support tickets, if you would like to do so, please contact us.

When you terminate your account on www.mentalhealthhub.com, all of your data will be erased. For information about Data Retention on CORDS, please see our CORDS Privacy Policy.

When you delete your data or terminate your account, it may still be stored with us for up to an additional 4 weeks due to the backups we have.

Right to object

You have the right to object to us using your data for marketing purposes. If you would like to do so, please contact us at. This will be done free of charge and without undue delay.

Communication from the site

We send all new members a welcoming email to verify their registration Established members may occasionally receive information on improvements to our service, general service announcements, and a newsletter. Out of respect for the privacy of our users, we present the option to not receive these types of communications.

Please see the Choice and Opt-out sections in the options menu on your account or the link provided in such emails.

On rare occasions, it is necessary to send out a strictly service-related announcement. For instance, if our service is temporarily suspended for maintenance, we might send users an email. Generally, users may not opt out of these communications; however, these communications are not promotional in nature.

We communicate with users on a regular basis to provide requested services and in regard to issues relating to their account, we reply via email or phone, in accordance with the user's wishes.

Retention Periods

We will retain your data for as long as necessary to carry out the service to you. If you wish to cancel your account, you should refer to the appropriate section in our terms of business/contract.

For CORDS, please see our CORDS Privacy Policy.

Privacy of Site Visitors

A "Site Visitor" is anyone who visits our site.

Cookies

We use both session ID cookies and persistent cookies. For the session ID cookie, once users close the browser, the cookie simply terminates.

A persistent cookie is a small text file stored on the Site Visitor's hard drive for an extended period of time.

Persistent cookies can be removed by following Internet browser help file directions (see below).

With session cookies, we are able to ensure that only people who have entered incorrect login details are able to use password-protected areas and only areas that they are authorised to use. Persistent cookies enable us to track and target the interests of our users to enhance the experience on our site. When you visit our site, we use cookies to store data on your device. This is so that we can:

- Distinguish you from other users of our website.
- Helps us to improve our website's performance and your experience of using our website
- Make it easier and more convenient for you to log in to our site, by storing the username and password on your device
- To track referral data and see how you got to our site
- To measure your usage of our services

Third-Party Cookies

Third parties we work with also place cookies on your device when you visit our website to provide you with marketing content which is tailored according to you, and in order to determine if such content is useful or effective. You can learn more about how to control cookies in your browser below.

How to control cookies from your web browser

Web browsers generally accept cookies. You can however change your setting to decline cookies. To learn more about this, please visit this link: www.aboutcookies.org/how-to-control-cookies

Do note that changing the setting on your browser to reject cookies means that you may not have access to important features on our site.

For more information about cookies applicable to www.mentalhealthhub.com, please see our Cookies Policy.

Right to complain

If you feel that we have mistreated the handling of your data, you have the right to complain to us in which case we will work with you to resolve the matter as quickly as possible and prevent any further mishandling.

You also have the right to complain to the Information Commissioner's Office.

Necessary disclosure by law

Though we make every effort to preserve user privacy, we may need to disclose personal information when required by law wherein we have a good-faith belief that such action is necessary to comply with a current judicial proceeding, a court order or a legal process served on our website.

Mental Health Hub

Mental Health Hub Cookies Policy

Cookie Policy

Information about our use of cookies. Our website uses cookies to distinguish you from other users of our website. This helps us to provide you with a good experience when you browse our website and also allows us to improve our site.

By continuing to browse the site, you are agreeing to our use of cookies.

A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer if you agree. Cookies contain information that is transferred to your computer's hard drive.

We use the following cookies:

- **Strictly necessary cookies.** These are cookies that are required for the operation of our website. They include, for example, cookies that enable you to log into secure areas of our website, use a shopping cart or make use of e-billing services.
- **Analytical/performance cookies.** They allow us to recognise and count the number of visitors and to see how visitors move around our website when they are using it. This helps us to improve the way our website works, for example, by ensuring that users are finding what they are looking for easily.
- **Functionality cookies.** These are used to recognise you when you return to our website. This enables us to personalise our content for you, greet you by name and remember your preferences (for example, your choice of language or region).
- **Targeting cookies.** These cookies record your visit to our website, the pages you have visited and the links you have followed. We will use this information to make our website and the advertising displayed on it more relevant to your interests. We may also share this information with third parties for this purpose.

(**Please note:** Third parties (including, for example, advertising networks and providers of external services like web traffic analysis services) may also use cookies, over which we have no control. These cookies are likely to be analytical/performance cookies or targeting cookies.)

You block cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, please note that if you use your browser settings to block all cookies (including essential cookies) you may not be able to access all or parts of our site.

Mental Health Hub

CORDS
Child Outcomes
Record Data System

CORDS Security Whitepaper

Organisational Security

Team training: All members of the Mental Health Hub team undergo quarterly security, privacy and compliance training and are required to complete questionnaires to assess their understanding. The safety and security of our user data is the responsibility of everyone in Mental Health Hub, therefore we ensure security training is included across every role and level of our organisation.

Access control to data: Access to the production environment and data is limited to senior management to reduce the risk of login exposure. Access (least privileged) is provisioned from centralised account management for Mental Health Hub to quickly respond to any compromised accounts. Any additional access granted to our team for production support is strictly on a need-to-know basis and removed when not needed.

Two Factor Authentication and Strong Password: CORDS maintains a strict password policy for logins to all internal or external services including production systems and tooling that CORDS use. It is mandatory for everyone in CORDS to create a strong and complex password with a 60-day rotation cycle and multi-factor authentication as a secondary login validation.

Incident and security response plan: Our focus at Mental Health Hub is to apply best security practices to safeguard our user data. In the event of any security incident, we have put in place a response plan to triage and resolve the problem as quickly as possible. If any data breach is detected, it is our responsibility to notify all affected users to help limit any further damage. Mental Health Hub strives to ensure similar incidents would not repeat by conducting post-incident reviews and implementing proper corrective and preventive steps.

Secure endpoints: Mental Health Hub has a stringent policy for the devices such as laptops and mobile devices used to access our tooling and services, we take appropriate precautions to keep them secure. Staff computers are locked with strong passwords, automatically locked when away and disks are encrypted by default. In the event of theft, an encrypted disk prevents anyone from reading the data and Mental Health Hub also enables remote location tracking and the capability to remotely erase data contained within those devices.

Application Security

Data encryption

In Transit

CORDS is built based on the client (your web browser) and server architecture. When using CORDS, web traffic between your web browser and servers is encrypted by using industry-standard TLS 1.2 protocols and AES256 encryption by default.

This secure connection prevents malicious actors from listening to your communications, tampering or forgery anywhere between your computer and our system.

At Rest

All information that is stored in the CORDS database is secured by AES 256-bit encryption. For highly sensitive data like patient identifiable information (PII), additional encryption is added to obscure the data. As a result, neither the database administrator nor third-party infrastructure staff can read the information.

File storage

Files such as any documents or attachments that were uploaded are encrypted using AES256 at rest and protected by access control (API level), which logically separates the file access from other CORDS users. Every file retrieval action is verified against the user's token to validate if it belongs to the owner.

Authentication (Password policy)

CORDS enforces a strong password policy when you or your client create an account. User passwords are then one-way hashed using AES256 to provide extra protection. A combination of hash and strong passwords will make it harder for brute-force attacks, such as using computational methods to guess the password. To combat this, our application detects any potential brute force activity such as too many failed login attempts and locks any high-risk accounts. Our system will automatically notify the affected users via email regarding suspicious activity.

Software development process and practices

At Mental Health Hub, we aim to catch security vulnerabilities in our development process and testing phase therefore our primary focus is to design our application with security in mind.

We incorporated security best practices in our development process via peer code review based OWASP leading industry-standard guidelines and methodologies (for example, checking on potential insecure endpoints or exposed access tokens). Private endpoints should only be accessible with valid access tokens and only return data that belongs to the owner.

Read more here: owasp.org/www-project-top-ten

We also use Synk (an industry-leading security and vulnerability scanning solution) as part of our development toolkit. Synk integrates directly into our development workflow allowing static code analysis, dependency scanning and more throughout our development process.

We have integrated dependencies and vulnerability scanning into our continuous delivery and build pipeline on third-party libraries. All development cycles go through our quality assurance checks and nightly automated regression tests in a staging environment before any deployment to production systems.

As part of an ongoing effort to stay up to date with cybersecurity trends, we conduct in-depth security reviews and workshops with our development teams.

Operations Security

Data centres

CORDS runs on top of Google Cloud utilising its world-class infrastructure and security. Mental Health Hub employs stringent security practices as per Google Cloud's recommendations to secure the access, data and production environments.

Google Cloud's data centres are also protected by multi-layered physical security such as 24/7 surveillance, multi-tiered controlled access to physical hardware and service availability supported by multi-availability zones. Operating systems, databases and services are regularly updated with the latest patches to remove any potential security vulnerabilities.

Network security

Mental Health Hub isolates testing and development environments from production systems to protect sensitive data. While engineers have access to testing and development environments, access to production systems is restricted to reduce compromised account-related risk.

Network security is a core part of overall security, especially towards detecting network intrusion. Mental Health Hub integrates firewall policies into our network (for example only whitelisting known IPs and only allowing essential network ports). All of our application services only allow system calls from known sources and with validated access tokens. Application system calls are logged and monitored. Alert policies are in place to detect potential intrusion.

Auditing and monitoring

Central to our security practices, auditing allows us to investigate who, when and what happened in the event of an intrusion. This is critical for our team to examine the scope of a data breach or security-related incidents which helps quickly take measures to close any security vulnerabilities and prevent similar events in the future.

Auditing is enabled for all of our production infrastructure and databases by logging database access, IP addresses, time and actions taken. These logs are stored securely for 30 days for analysis and to aid any backdated investigations if needed.

Monitoring prevents potential threats from happening by alerting our tech team to take appropriate steps to respond to malicious actors. Mental Health Hub deploys multiple alerting systems around our application and network to reduce downtime and provides our tech team with the context to troubleshoot and resolve any technical issues. All application system calls are recorded and alert policies are set up to notify our technical team when incidents are raised. We actively prioritise our investigation into these alerts to resolve any technical issues and prevent any malicious activities.

To safeguard our user's account, all CORDS logins events are logged to detect any unusual traffic or pattern such as multiple failed login attempts. Too many failed attempts will result in an account being blocked to prevent any password brute force attack. In addition, our technical team will be notified so we could assess if it is a legitimate login issue and help to unblock these users when needed.

Disaster recovery and business continuity

CORDS employs several mechanisms to ensure high availability and resiliency. CORDS services are hosted on the Google Cloud platform in the United Kingdom. CORDS service infrastructures are able to self-heal by replacing degraded servers with new instances. Servers are also load-balanced with multiple instances and deployed across multiple availability zones.

Customer data is stored regionally in Amazon Web Services (AWS) data centres which are designed to be highly redundant and replicated across different servers to improve scalability and availability.

This also enables zero downtime in the event of server patches and maintenance.
The database platform is also fault-tolerant and has the capability to automatically failover to healthy servers so our services can continue to operate without interruption.

We treat data integrity and availability as just as important. To protect your data against data-related failure or data corruption, Mental Health Hub has established thorough backup policies for our databases. Your data is constantly backed up every 2 hours, weekly and monthly. These backups are also stored securely independently from the infrastructure the database resides on.

Data Ownership

CORDS is a **Data Processor** while **you** are the **Data Controller**. This means your data is yours, we don't scan it for marketing or advertising nor sell it to third parties.

In line with our Software License Agreement, we may create data that is de-identified in accordance with our Privacy Policy. This de-identified information is not Personal Information, because it cannot be used to identify any individual, and may be used by us to help us improve our products and services.

Mental Health Hub customers retain the rights to their data ownership. If you request to migrate to another system, we can support you by enabling you to make a copy of all your data to move securely.

If a request for data erasure is made, Mental Health Hub will take appropriate steps to mark the data for deletion. Access to the data will be immediately made unavailable and any deletion or removal is done in accordance with our privacy policy.

Key Policies

Adherence to all of the required legislation and government guidance. As a UK company, Mental Health Hub complies with the specific rules and regulations for the locations in which we operate in relation to the way we gather and handle data. In the UK, we adhere to GDPR and the Data Protection Act.

The details are outlined in our Software License Agreement, Data Sharing Agreement and Privacy Policy.

Data Residency

Mental Health Hub ensures all customer data resides and is processed 'on shore' in their country of origin. This policy extends to third-party service providers we use. For UK customers, data is stored in London data centres.

Third-Party Processors

To provide you with the very best service CORDS partners with world-leading technology partners to enable some of our software capabilities.

We conduct a rigorous assessment of the security of our third-party providers to ensure they employ appropriate levels of security, compliance and privacy policies.

We work with the following, highly reputable providers.

Provider	Services	Security Information
Tacklit	Software development, engineering and cloud infrastructure	tacklit.com/security
Google Cloud Platform	Cloud infrastructure	cloud.google.com/security
AWS	Cloud infrastructure	aws.amazon.com/security
Auth0	Account management	auth0.com/security
MongoDB	Data storage	docs.mongodb.com/manual/security
Twilio	SMS and other messaging	twilio.com/legal/security-overview
SendGrid	Email	sendgrid.com/policies/security
Helpscout	Online customer support	helpscout.com/company/legal/security
Sentry	Application error monitoring	sentry.io/security
Stripe	Payment processing	stripe.com/docs/security/stripe
Wonde	Secure data transfer and School MIS connection	wonde.com/security
HubSpot	Customer relationship management	legal.hubspot.com/security

CORDS Privacy FAQs

This forms part of the application process to use relevant Mental Health Hub Products.

The Headteacher or an authorised member of staff will agree to have read and understood the terms and conditions outlined below:

Who is responsible for managing my information?

CORDS is provided by the Mental Health Hub and its suppliers.

Mental Health Hub is responsible for ensuring that your data is adequately protected in relation to the operation of CORDS.

Who can I contact if I have queries about this privacy policy?

Please contact us directly.

Will you ever update this privacy policy?

We may update this privacy policy from time to time and we will send a notification to your main account contact if this is the case.

How can I update my data?

The data in CORDS reflects the data in your school MIS system, hence, to correct any inaccuracies you should correct the data in your MIS and allow an overnight update to occur.

If it is important that data changes are shown more urgently (for example, if a parent has been restricted from contact with their child by court order) then you can contact us for assistance.

What information do we collect?

We collect student and staff information such as names, record identifiers and contact details. The full information we collect is detailed in the section entitled "Transfer and Use of Personal Information", above.

What is my information used for in CORDS?

The information stored on CORDS is used to enable the customer to issue surveys and collect responses to questions. You can do many things in CORDS, like run reports to view the information collected to analyse performance/improvement.

How is my information held within CORDS?

The data is stored on CORDS using reputable companies and industry-standard technology to ensure that the information is kept safe.

How long will my information be held for by CORDS?

The information on CORDS will be held for the duration of the contract/term that the customer has signed up to and for 12 months thereafter.

How do I delete my data from CORDS?

In order to terminate your account with CORDS, you must contact us in writing, expressing your wish to stop using CORDS.

Mental Health Hub

CORDS Privacy Policy

About CORDS

The purpose of CORDS is to provide tools and services to schools that empower them with the technology and support to create an effective whole-school approach to mental health, undertake universal screening to prevent and identify mental health conditions and more accurately measure the impact of interventions and support through world-leading outcome measures.

INSERT INFO from Bounce Together DPIA.

We collect, store, and use your data on our servers to provide you with the ability to better maintain and improve your Services. We may also use data in an aggregated and de-identified form for our own purposes.

Information We Collect

We collect such information regarding our users and their interactions with our Services. We will collect relevant and necessary information depending on the nature of your relationship with our Services. For parts of our Service, through connecting CORDS users and other individuals, we act in the role of the Data Processor while you are the Data Controller.

Where any data is requested from another individual by a CORDS user via a tool, survey, assessment or another request via our Services, you are responsible for making sure that those individuals' privacy and associated rights are respected.

As your Data Processor, we will take care to protect the privacy of these individuals associated with your setting and will process their Personal Data in accordance with the terms of the CORDS Software Licensing Agreement

Broad categories:

- **Student Data:** Such as MIS Record number (Student ID), Forename, Surname, Gender, Date of Birth
- **Staff Data:** Such as Forename, Surname. School Email, Record number (Staff ID), Gender, Current Employee Status
- **School Details:** Such as School Name, Education Phase, Address, DfE ID

Data Exported via Wonde

Class Data

Classes alternative read
Classes code read
Classes description read
Classes name read
Classes read
Classes subject read

Contacts Data

Contacts address read

Contacts details read

Contacts email notification read

Contacts email read

Contacts forename read

Contacts gender read

Contacts initials read

Contacts lives with pupil read

Contacts middle names read

Contacts parental responsibility read

Contacts priority read

Contacts read

Contacts relationship read

Contacts salutation

Contacts surname read

Contacts telephone read

Contacts title read

Contacts UPI read

Employee Data

Employee read

Employees contact details read

Employees current read

Employees date of birth read

Employees email read

Employees employment details read

Employees employment end date read

Employees employment start date read

Employees forename read

Employees gender read

Employees initials read

Employees middle names read

Employees role text read

Employees staff code read

Employees surname read
Employees teacher number read
Employees teaching staff read
Employees title read
Employees UPI read

Group Data

Groups code read
Groups description read
Groups division read
Groups name read
Groups notes read
Groups read
Groups type read

Medical Data

Medical Conditions date received read
Medical Conditions description read
Medical Conditions severity read
Medical conditions read

Photo Data

Photo read
Photos content read
Photos person id read
Photos person type read

SEN Data

SEN category code content read
SEN category description content read
SEN description content read
SEN end date content read
SEN rank content read
SEN start date content read
SEN type code content read

SEN type description content read

Student Data

Special education needs read
Student absences absence type read
Student absences authorised by read
Student absences comment read
Student absences end at read
Student absences event type read
Student absences read
Student absences reason read
Student absences start at read
Student absences student id read
Students English as additional language read ***(Optional)***
Students English as additional language status read ***(Optional)***
Students SEN read
Students UPN rea
Students contact details read ***(Optional)***
Students cultural read
Students date of birth read
Students demographics read
Students education details read
Students email read ***(Optional)***
Students ethnicity code read
Students ethnicity read
Students ever in care read ***(Optional)***
Students first language read ***(Optional)***
Students forename read
Students former UPN read
Students gender read
Students identifiers read
Students in LEA care read
Students in care details read
Students initials read
Students middle names read

Students permissions read ***(Optional)***
Students photograph student read ***(Optional)***
Students premium pupil indicator read
Students premium pupil notes read ***(Optional)***
Students read
Students surname read
Students unique
Learner number read
Students UPI read
Wellbeing data read
Wellbeing mental health risk data read
Students premium pupil eligible read

There are some elements of your Personal information that are deemed sensitive in line with the Data Protection Act. Sensitive information is a subset of personal information that is given a higher level of protection under the Data Protection Act. This includes information relating to recording a person's physical or psychological health for the purposes of assessing, maintaining, improving or managing the person's health.

The type of necessary health information we may collect and hold due to the nature of our Service includes.

- Details of presenting symptoms as reported by a CORDS user and/or another individual
- Details of any referral from another health service
- Outcome measurement data through the completion of assessments

Collecting Data

There are two primary ways we collect information.

A. We collect information through your use of our Services. When you visit or use our Services, including when you browse the Sites or Apps, register a User Account, and use the Software, we will usually gather and collect such uses, sessions and related information, either independently or with the help of third-party services, including through the use of "cookies" and other tracking technologies.
B. We collect information provided by you. For example, we collect the Personal Information you provide us when you register for our Services; when you submit or upload such Personal Information as you use any of our Services; and/or when you contact us directly by any communication channel, for example reaching our team to help you resolve a query.

Cookies and Web Beacons

We may use cookies on our Site from time to time. Cookies are text files placed in your computer's browser to store your preferences. Cookies, by themselves, do not tell us your email address or other personally identifiable information.

However, they do allow third parties, such as Google and Facebook, to cause our advertisements to appear on your social media and online media feeds as part of our retargeting campaigns. If and when you choose to provide our Site with personal information, this information may be linked to the data stored in the cookie.

We may use web beacons on our Site from time to time. Web beacons (also known as Clear GIFs) are small pieces of code placed on a web page to monitor the visitor's behaviour and collect data about the visitor's viewing of a web page. For example, web beacons can be used to count the users who visit a web page or to deliver a cookie to the browser of a visitor viewing that page.

We use Google Analytics to help us understand how users engage with our Services. Google Analytics uses cookies, web beacons and other technologies to track your interactions with our Services, then collects that information and reports it to us, without identifying individual users. This information helps us improve our Services so that we can better serve users like you.

Please refer to our Cookies Policy.

How we use your information

We process your information in line with the principles of the UK GDPR and (where applicable) the EU GDPR and the Data Protection Act. We process your personal data on a lawful basis by asking for your explicit consent to do so, or in line with our contractual obligation to you.

Where the legal basis for us processing your personal data is that you have provided your consent, you may withdraw your consent at any time. You will not suffer any detriment for withdrawing your consent. If you withdraw your consent, this will not make the processing which we undertook before you withdrew your consent unlawful.

You can withdraw your consent at any time by contacting us.

By using our Service, you consent that we may use your information in the following ways:

Provide you with the Services and fulfil your requests: We may use your information to register you, administer your account, and provide you with the information, products and services that you request. For example, we respond to your questions when you contact us, and assist with any problems you report about our Services.

Enhance your experience: We use your information to personalise and enhance your experience when you use the Services, for example remembering preferences or showing you applicable recommendations.

Communicate with you: We may contact you via email, phone, SMS, push notification or other applicable messaging services as part of our overall product experience in sharing relevant information with you. We may also share information and materials that we think might be of interest to you, including information about products and services that promote health and wellness. You may unsubscribe from receiving communications about these products and services by using the unsubscribe and notifications settings in your profile, through the unsubscribe link in an email, or by contacting us.

Improve our Services: Your information helps us improve the content and functionality of our Services. For example, we may conduct measurement activities and analyse trends, usage and activities in connection with the Services to create new features and content to aid our Users.

Protect CORDS and our Users: We may use information about you to detect, investigate and prevent fraudulent transactions and other illegal activities and protect the rights and property of CORDS and others.

Creation of De-Identified Information: We may use your Personal Information to create data that is de-identified in accordance with the Data Protection Act. This de-identified information is not Personal Information, because it cannot be used to identify you, and may be used by us for any lawful purpose.

In addition to those purposes listed above, we may use your information for any other purpose disclosed to you at the time of collection.

Disclosure of personal information

We may disclose personal information to:

- **CORDS users (if you are an individual):** Including school teachers and support staff who evaluate mental health assessments and track interventions in line with our Software Licensing Agreement
- **Reporting:** Summary of mental health data may be anonymised and aggregated for national and industry reporting.
- **Other Service Providers:** Including payment system operators; and third-party hosting and information security providers that provide computer, storage and information security resources to CORDS.
- Anyone to whom our business or assets (or any part of them) are, or may (in good faith) be, transferred.
- Courts, tribunals, regulatory authorities and law enforcement officers, as required by law, in connection with any actual or prospective legal proceedings, or in order to establish, exercise or defend our legal rights.
- In addition, where it relates to sensitive health information, in line with the permitted health situations detailed in the Data Protection Act we reserve the right to use or disclose such information where we reasonably believe it is necessary to prevent a serious threat to life, health or safety. Any such disclosure will be done in accordance with the Data Protection Act.

By sharing your school's information with us, you acknowledge that we utilise third-party cloud services to manage our systems providing you data processing services. As a result, some of your data may be hosted in the UK, EU, AU or US.

We work with data processors who have stringent data protection policies in place to support the data protection requirements of Schools using CORDS. While these processors are committed to maintaining the strict confidentiality and protection of personal and mental health-oriented data, it's important to note that these protected systems may process or store data in multiple countries first world countries.

Examples of **third-party processors** include Microsoft Azure, Amazon AWS, Google Cloud Platform, IBM Cloud and system developed on these highly respected cloud providers. Our list of third-party processors can be found on **page 23** of this document.

We never sell personal data and we carry out all processing operations in compliance with the General Data Protection Regulation ("GDPR"). **We may share de-identified information and other de-identified non-personal Information in all legally permissible ways.**

Links to other websites: Note that while our Services may contain links to other websites or services, we are not responsible for such websites or services' privacy practices. We encourage you to be aware when you leave our Services and read the privacy statements of each and every website and service you visit before providing your Personal Information. This Privacy Policy does not apply to such linked third-party websites and services.

Storage and Security

We are committed to ensuring that the personal information we collect is secure. To prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the personal information and protect it from misuse, interference, loss and unauthorised access, modification and disclosure.

We cannot guarantee the security of any information that is transmitted to or by us over the Internet. The transmission and exchange of information are carried out at your own risk. Although we take measures to safeguard against unauthorised disclosures of information, we cannot assure you that the personal information we collect will not be disclosed in a manner that is inconsistent with this Privacy Policy.

Data Retention

We will retain your personal data for a **period of twelve months after our relationship with you has ended**. After this period, your personal data will be anonymised or deleted, as per our CORDS Software Licensing Agreement.

For CORDS users, you are solely responsible as Data Controller for retaining any required information or records in line with statutory requirements relating to retaining medical records for minimum terms.

If you leave our Service, you are able to download all data you have stored on our software to store it elsewhere if you should so require.

We will not store your personal data for longer than is reasonably necessary to use it in accordance with this Privacy Policy or with our legal rights and obligations. For the avoidance of doubt, aggregated and anonymised data and any information other than personal data can be stored indefinitely.

Controlling your personal information (Your legal rights)

- **Choice and consent:** Please read this Privacy Policy carefully. By providing personal information to us, you consent to us collecting, holding, using and disclosing your personal information in accordance with this Privacy Policy. You do not have to provide personal information to us, however, if you do not, it may affect your use of this Site or the products and/or services offered on or through it.
- **Information from third parties:** If we receive personal information about you from a third party, we will protect it as set out in this Privacy Policy. If you are a third party providing personal information about somebody else, you represent and warrant that you have such a person's consent to provide the personal information to us.
- **Restrict:** You may choose to restrict the collection or use of your personal information. If you have previously agreed to us using your personal information for direct marketing purposes, you may change your mind at any time by contacting us using the details below.
- **Access:** You may request details of the personal information that we hold about you, this legal right is protected by the Data Protection Act 2018 and UK (and EU where appropriate) General Data Protection Regulations.
- **Correction:** If you believe that any of the information we hold about you is inaccurate, out of date, incomplete, irrelevant or misleading, please contact us using the details below. We will take reasonable steps to correct any information found to be inaccurate, incomplete, misleading or out of date.
- **Complaints:** If you believe that we have breached the Data Protection Act and wish to make a complaint, please contact us using the details below and provide us with full details of the alleged breach. We will promptly investigate your complaint and respond to you, in writing, setting out the outcome of our investigation and the steps we will take to deal with your complaint.
- **Unsubscribe:** To unsubscribe from our email database or opt out of communications (including marketing communications), please contact us using the details below or opt out using the opt-out facilities provided in the communication or via your user profile.

If you tell us you want to exercise your rights, we'll confirm that we have received your request and let you know if we need anything else from you, then we will respond as quickly as possible and, in any case, within a month.

Mental Health Hub

CORDS
Child Outcomes
Record Data System

CORDS Data Sharing Agreement

Introduction and Aims

This document details the data objects and items that are shared, the use of, use by, methods, storage, storage duration, safeguarding and security of the data that **you** (the '**customer**') agree to share with **us** (**Mental Health Hub**) (the '**company**').

Definition and Interpretation

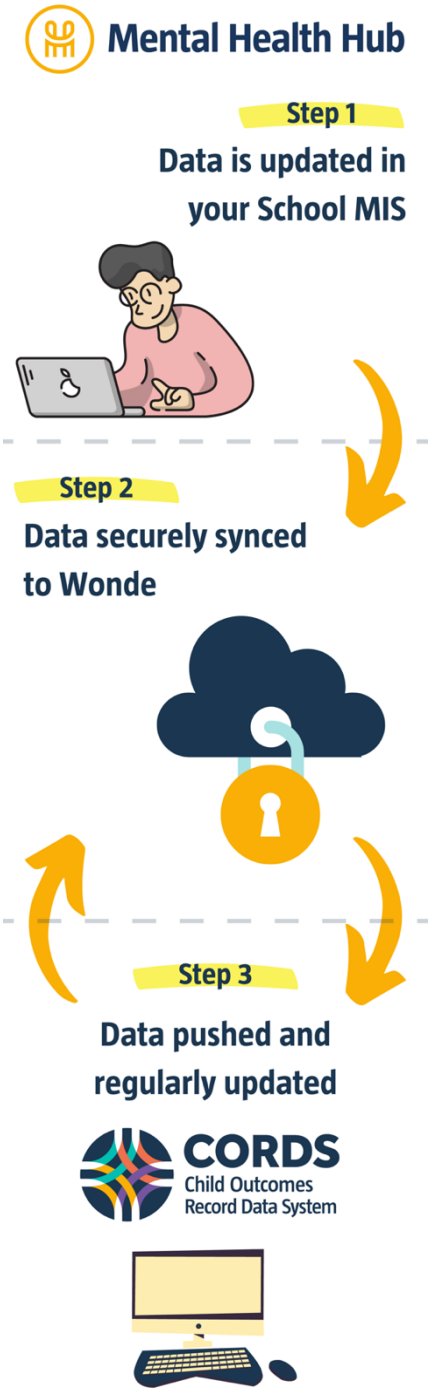
In this agreement, the following words and phrases shall have the following meanings (unless the context otherwise requires).

Term	Definition
"DPA", "the Act" or "GDPR"	Refers to the Data Protection Act 2018, General Data Protection Regulations (GDPR) and all applicable laws and regulations relating to the processing of personal data and privacy.
"CORDS"	CORDS is an online provision coordination software that enables you to capture and analyse data through the use of online surveys. This software is provided by Mental Health Hub.
"Data controller", "Data processor", "Personal data" and "Processing"	Retain the legal definitions provided to them in the Data Protection Act and GDPR.
Mental Health Hub	The company and provider of CORDS.
"School Management Information System" or "MIS"	The software used by schools to manage their student and staff data. Popular examples for schools include SIMS and Arbor.
"School" or "Customer"	Refers to the education provider or other organisation that the Mental Health Hub provides CORDS to.
Wonde	A solution for education providers to securely collect and deliver data to one or more selected partners. Used by the Department for Education data collection on attendance.

Overview of Data Movement

In order for CORDS to be of significant use, it must be provisioned with your school's user data.

This section gives details of the movement and storage of data between your School MIS and CORDS when you consent to share your data.

<table>
<tr>
<td rowspan="3"> 
</td>
<td>Wonde facilitates the extraction of data between your School Management System and CORDS.

In this first step, Wonde configure your School Management System to sync with the Wonde dashboard.</td>
</tr>
<tr>
<td>Wonde will not allow the transfer of data to CORDS by default.

You must specifically give permission via your school's Wonde dashboard to allow sharing to occur.

Wonde calls this step an Authorisation and the extent of Personal Information shared with CORDS is governed by this authorisation.
For the purpose of CORDS, the data shared is outlined in full detail in the section "Data to be transferred".</td>
</tr>
<tr>
<td>An Authorisation in Wonde allows a specific list of data areas to be read, for a specific partner that you gave Authorisation to.

When you give consent, the permission for the movement of data within the scope of that Authorisation is perpetual until you, CORDS, or Wonde withdraws it.</td>
</tr>
</table>

Revoking Access

Your school's Wonde dashboard also enables you to revoke permission from CORDS.

When you revoke permission, you must specify an end date for that sharing and Wonde will cease allowing access by CORDS from that date.

If you retrospectively revoke permission, data access may continue for up to 72 hours.

Withdrawing authorisation for the movement of optional data to be read/written by CORDS does not end your commercial relationship with us.

If you do withdraw consent for data transfer for CORDS or required data, then you do need to remember that this may impact some or all service(s) or contract(s) that you have in place with the Mental Health Hub.

If you are unsure of any implications, please contact us.

Wonde Integration Process

Process from Wonde

Please see www.wonde.com for more information.

1. CORDS requests access to school data

CORDS can only request the exact data that we need. Wonde calls these permissions - the school is always in control of them.

2. School is notified of the CORDS request

Wonde will let the school know that CORDS is requesting access to specific data. The school logs in to the secure Wonde dashboard to view all pending requests.

3. School controls the request via Wonde

The school can review the data requested by CORDS. Once they are happy with the request, the school can approve, decline or revoke the request.

4. Integration is complete

The exact data flows through to CORDS safely and securely. The school is ready to access and enjoy access to CORDS.

The school will always have total control over the data they share. Support from Wonde is available through every step of the process.

Use and Processing Data

This section and document are provided for schools to ensure that, as data controllers, they have transparency over the data that is being shared and that they consider there to be appropriate measures in place, to ensure that the data is held securely and confidentially. This section provides information to support these objectives.

Mental Health Hub and its suppliers will be acting as data processors as defined by the Act and we have taken all reasonable measures to ensure the safety and security of personal information and continues to review these measures on an ongoing basis.

Data to be transferred

To enable you to use all functions of CORDS, we require the transmission/sharing of specific information from your MIS.

Data shared

(Note: The fields listed under the "School Details" heading are not categorised as personal data but are included for your information)

Broad categories:

- **Student Data:** Such as MIS Record number (Student ID), Forename, Surname, Gender, Date of Birth
- **Staff Data:** Such as Forename, Surname. School Email, Record number (Staff ID), Gender, Current Employee Status
- **School Details:** Such as School Name, Education Phase, Address, DfE ID

Please see the next page for the comprehensive list of data exported and shared via Wonde.

Data Exported via Wonde

Class Data

Classes alternative read

Classes code read

Classes description read

Classes name read

Classes read

Classes subject read

Contacts Data

Contacts address read

Contacts details read

Contacts email notification read

Contacts email read

Contacts forename read

Contacts gender read

Contacts initials read

Contacts lives with pupil read

Contacts middle names read

Contacts parental responsibility read

Contacts priority read

Contacts read

Contacts relationship read

Contacts salutation

Contacts surname read

Contacts telephone read

Contacts title read

Contacts UPI read

Employee Data

Employee read

Employees contact details read

Employees current read

Employees date of birth read
Employees email read
Employees employment details read
Employees employment end date read
Employees employment start date read
Employees forename read
Employees gender read
Employees initials read
Employees middle names read
Employees role text read
Employees staff code read
Employees surname read
Employees teacher number read
Employees teaching staff read
Employees title read
Employees UPI read

Group Data

Groups code read
Groups description read
Groups division read
Groups name read
Groups notes read
Groups read
Groups type read

Medical Data

Medical Conditions date received read
Medical Conditions description read
Medical Conditions severity read
Medical conditions read

Photo Data

Photo read
Photos content read

Photos person id read

Photos person type read

SEN Data

SEN category code content read

SEN category description content read

SEN description content read

SEN end date content read

SEN rank content read

SEN start date content read

SEN type code content read

SEN type description content read

Student Data

Special education needs read

Student absences absence type read

Student absences authorised by read

Student absences comment read

Student absences end at read

Student absences event type read

Student absences read

Student absences reason read

Student absences start at read

Student absences student id read

Students English as additional language read ***(Optional)***

Students English as additional language status read ***(Optional)***

Students SEN read

Students UPN rea

Students contact details read ***(Optional)***

Students cultural read

Students date of birth read

Students demographics read

Students education details read

Students email read ***(Optional)***

Students ethnicity code read

Students ethnicity read

Students ever in care read ***(Optional)***

Students first language read ***(Optional)***

Students forename read

Students former UPN read

Students gender read

Students identifiers read

Students in LEA care read

Students in care details read

Students initials read

Students middle names read

Students permissions read ***(Optional)***

Students photograph student read ***(Optional)***

Students premium pupil indicator read

Students premium pupil notes read ***(Optional)***

Students read

Students surname read

Students unique

Learner number read

Students UPI read

Wellbeing data read

Wellbeing mental health risk data read

Students premium pupil eligible read

Data Life Cycle

Your data's point of origin remains in the school MIS, which means the school is responsible for the quality of the data that is being shared. Any of the changes that you do make in the MIS, will be synchronised to CORDS as described below.

New 'personal' records

When a new staff or student record is detected in the MIS and meets the selection criteria it will be uploaded to CORDS at the next transmission and appear in the user interface accordingly for authorised users.

Changed 'personal' records

When an updated staff, student or contact record is detected in the MIS, and meets the selection criteria it will be updated in CORDS at the next transmission and appear in the user interface accordingly for authorised users.

Deleted 'personal' records

When a staff, student or contact record in the MIS no longer meets the selection criteria or is deleted, this data stops being transmitted to CORDS.

When a person is detected as deleted or left, CORDS immediately revokes permissions for that person and retains their historic activity indefinitely to provide an audit.

New group memberships

When a person is detected to have a new or changed group membership (for example a registration group, staff post, etc.) this will be notified to CORDS on the next transfer and will then be reflected in the user interface for authorised users.

Deleted or ended group membership

When a person is detected to have left a group membership (for example a year group, class group, etc.) this will be notified to CORDS on the next transfer and will then be reflected in the user interface for authorised users.

Data Storage and Security

The information from your school is held inside CORDS, which is hosted within the United Kingdom

Every effort is made to ensure the data held by CORDS is secure and our reputable hosting provider applies a variety of techniques to ensure the data is kept safe.

In terms of the data sharing between CORDS and Wonde, the data is securely uploaded using industry-standard SSL encryption and a unique identifier configured in Wonde ensures that the information is linked to the correct customer account on CORDS.

Wonde accesses your school MIS system using credentials that you provide and cannot access it without them.

For more information about the security policies that apply to CORDS, please contact us

Support

The team at Mental Health Hub are able to resolve or advise you on any technical issues that you encounter while using our products and provide first-line support for the Wonde integration also.

Occasionally it can be necessary for our team to view the issue with you, in order to diagnose it fully and offer a solution.

In circumstances where this needs to be viewed remotely, they may use remote access tools to view your computer with you, in which case you should remain at your computer and supervise the entire session.

All of our remote sessions allow you to retain control and allow you to terminate the session at any time.

If your issue escalates and an additional support technician is required, then they may also be invited to join the remote session.

In some cases where a second-line escalation is required for Wonde, this may involve also allowing a Wonde support technician to join the remote session.

If your issue is a software issue or requires changes to your account configuration, then Mental Health Hub staff may perform such configuration on your behalf from our secure management software without the requirement for remote access.

You are reminded that you should avoid sending personal information, such as student/contact records, to us directly via email.

You certainly should only send such information when supported by strong encryption, if there is an explicit requirement to do so.

The Mental Health Hub team will advise the most secure method for transfer if there is such an explicit requirement.