OSA
Online Safety Alliance

Data Protection and Privacy Policy

The web presence of the Online Safety Alliance is managed by What2Learn Ltd. What2Learn Ltd is registered with the Information Commissioner's Office. What2Learn Ltd and the OSA aim to be as clear as possible about how and why we use information about you so that you can be confident that your privacy is protected. This policy describes the information collected when you use OSA services. This information includes personal information as defined in the General Data Protection Regulation (GDPR) 2016 (and the subsequent UK Data Protection Bill enacted in 2018).

The online presence of the OSA consists of two distinct components. The blog-based system is powered by WordPress and collects no user data and places no cookies on user systems.

The Moodle-based system (all URLs starting with https://certificate.onlinesafetyalliance.org) does require collection and use of user data and cookies as detailed below.

Third-party ad servers

There are no third-party ad servers or ad networks used at onlinesafetyalliance.org and no user data is shared with any third parties.

Log Files

The OSA's Moodle-based system makes used of log files. The information inside the log files tracks interaction with elements within the online safety courses and scores attained in assessments. This data is essential to collect to measure user progress towards completion of the course. No Analytics-style data is collected on user location and search history.

Cookies and Web Beacons

The Moodle-based system of the OSA uses Session Cookies. A session Cookie is generated when you log into the Certificate system. A session cookie only holds information for that session. When you log out this cookie is removed.

Some sections of the Moodle-based system require students to visit highly reputable external websites such as the NSPCC and ThinkUKnow. These external sites are not controlled or managed by What2Learn Ltd and may use cookies. The privacy policies of these external sites should be considered separately to this policy.

If you wish to disable cookies, you may do so through your individual browser options. More detailed information about cookie management with specific web browsers can be found at the browsers' respective websites. It must be noted that this will prevent a user from being able to record scores achieved in assessments and will thereby prevent successful completion of the Certificate.

Customer data

No data is collected or stored by the OSA system which could be considered ‘high risk’.

What student data is stored?

Data minimisation is given a high priority. Student data stored in the OSA Moodle-based system is first and last name and school year. Students are assigned to school-based groups. Schools have the option of including an email address for their students to enable them to reset their own password. Password resets are the only time we would send a student an automated email and the only way in which we use student email addresses stored on our systems. Log data as defined above is also collected. On no occasion do we disclose student information to other parties.

Our understanding is that schools are permitted to pass on student names and emails to us, on the basis that they are doing so to further the educational needs of their students. This includes students under 13 where the school is acting in logo parentis. If students do not have an email address linked to their account, they will need to ask a teacher to request their password is reset.

What teacher data is stored?

Teacher data stored in the OSA Moodle-based system is name and email address. We require each teacher account to have an email address to allow passwords to be reset and to allow us to communicate changes to the site and to provide administrative support. Log data as defined above is also collected.

Where school staff have signed up to the OSA email newsletter in order to receive free access to the Moodle-based CPD course for school staff, additional information is collected. Additional data collected is employer name, role in school and school phase. This data is stored with the service MailChimp to ensure full GDPR compliance. MailChimp’s data privacy documentation can be seen at https://mailchimp.com/legal/privacy/. This data is used for very occasional email communications relating to online safety issues or OSA services that the OSA believes might be of interest to school staff. This data is not shared with any third parties and the individual may unsubscribe from such communications at any time.

Who can access the data?

Student progress data is only accessible to teachers at the student’s school and to OSA administrators managing the system. All employees who have access to user data are trained on their responsibilities in line with current data protection legislation.

Where is the data stored?

All user data is kept on a pair of secure databases, and a web server. All data is stored within the EU using Amazon Web Services (AWS) based in Ireland. For full details of how AWS ensure GDPR compliance please visit https://aws.amazon.com/compliance/gdpr-center/

Data security

HTTPS is used on the servers and throughout the OSA online presence to encrypt and secure the data of those using the OSA system. Administrative access to systems is provided to limited to key individuals and complex administrative access codes are employed to reduce the threat of unauthorised access. Administrative access to the system is monitored through log data. Daily backups of user data are kept on servers and tested to ensure timely restoration of user data in the event of a physical or technical incident. All systems and software are maintained with relevant security updates. In the event of a data breach being identified, the Supervisory Authority would be contacted within 72 hours along with the nominated point of contact within each affected school. Repeated failures to access the System result in automated IP banning and temporary account lockouts.

Data shared between establishments and What2Learn Ltd is encrypted with passwords shared through alternative communications channels.

Data security procedures are regularly reviewed.

Legal basis

We shall only process your Personal Data in accordance with principles of data protection and if there is a legal basis to do so. Data processed by onlinsafetyalliance.org meets the principles of Legitimate Interest within the GDPR as:

- Data is processed to support the development of knowledge relating to online safety issues in children and school staff (a Statutory requirement within 'Keeping Children Safe in Education', DfE 2016).
- Processing of data is necessary to verify and record that individuals have successfully demonstrated knowledge of online safety issues.

Data Retention

Unless we receive a deletion request, we will retain your information for as long as your account is active or as is reasonably useful for operational purposes.

Personal Privacy

Students are not visible to one another and our systems do not permit messages to be sent between any users.

Use of Integrated Services

Some users may opt to use Google or Microsoft Integrated Services to gain access to the Moodle-based system of onlinesafetyalliance.org using existing account details. Doing so will grant onlinesafetyalliance.org access to basic profile information to with the sole purpose of identifying users to record their progress through our learning materials and assessments. Our product uses

OAuth 2 for user authentication and the user is informed clearly of the level of access they will be providing and the purpose of this access. We never have access to Google or Microsoft passwords.

In using OAuth 2, What2Learn Ltd is compliant with:

- The Developer Policy of Google Platform
- The Policy of Google Buttons
- The EU User Consent Policy

You may revoke our access to your account on any Integrated Service, such as Google or Microsoft, at any time by updating the appropriate settings in the account preferences of the respective Integrated Service. You should check your privacy settings on each Integrated Service to understand and change the information sent to us through each Integrated Service. Please review each Integrated Service's terms of use and privacy policies carefully before using their services and connecting to our system.

Use of integrated services is optional and down to the preference of each school. Where Integrated Services are not used accounts will be created for teachers and students in a format agreed with a designated member of school staff.

Right of Erasure

In accordance with applicable European legislation you can delete your account and your usage logs from the system. In the case of requests to delete student accounts, the relevant school will be informed that this request has been made in order to confirm that the request made is legitimate.

Your rights

You have the right to exercise your data protection rights at any time.

You have the right to request information as to the personal data relating to you has been processed by us.

Contact person

If you have questions regarding data protection, need information or want your data to be deleted please contact our Data Protection Officer via email: privacy@onlinesafetyalliance.org