

Information & Cyber Security Policy for Colleges and Schools

Review date: October 2027

Why we have this policy

The Day works with schools and colleges to provide digital learning and wellbeing resources to young people. This policy explains the measures we use to protect college and student information when it is handled through The Day's services. It is intended to give colleges a clear and practical view of how we protect student data, control access to the platform and support safeguarding.

This policy should be read alongside the relevant Data Processing Agreement, the Website Privacy Notice, the Information & Cyber Security Policy and our Safeguarding Policy. Where a college is the data controller and The Day acts as its processor, the DPA sets out the specific processing arrangements, responsibilities and instructions that apply to that relationship.

Scope

This policy applies to student and college information processed through The Day's services, including account information, assessment and poll responses, platform activity and information used to support the delivery and evaluation of our products.

It covers information processed for participating colleges and the controls used by The Day employees and service providers when supporting those services.

Our security and safeguarding commitments

The Day is Cyber Essentials certified. We use recognised security controls and practical safeguards designed to protect information from unauthorised access, loss, misuse or disruption.

Our approach is based on least-privilege access, strong authentication, secure systems, appropriate data minimisation and prompt response to security or safeguarding concerns. Safeguarding is treated as an organisational responsibility and is supported by the platform design, access controls, moderation arrangements and clear routes for raising concerns.

Access to the platform

Access to The Day's platform is controlled so that only authorised users can log in. Depending on the college's configuration, users authenticate through single sign-on (SSO) or multi-factor authentication (MFA). We do not rely on a simple password-only login where SSO or MFA authentication is required for the relevant service.

Each user should have their own account. Access is limited according to role and organisation. College administrators and teachers can access the student information they need for the purposes of managing and supporting their students. The Day staff only receive the level of access necessary to provide and support the service.

Student information and visibility

Student information is designed so that it is visible within the school or college organisation to authorised teachers and administrators who need it for the service. Students do not receive access to other students' private information.

For The Day's administrative users, student records are pseudonymised. The Day admin view uses a randomly generated username rather than showing the student's real name as part of routine administration. This helps limit direct identification while allowing the platform to operate and support the service.

Student data stored securely

Student data is stored in an AWS database within our managed technology environment. Access to the underlying data and systems is restricted to authorised personnel and service providers with a legitimate operational need, and security controls are applied to protect against unauthorised access, alteration or loss.

The Day regularly reviews its security arrangements and will take proportionate steps to respond to identified risks, incidents and changes to the services we provide.

What information we collect and why

The exact information collected depends on the service and the configuration agreed with the school or college. Student information may include a randomly generated username and responses or activity data created through use of the service.

We may also request gender and month and year of birth for students where this is needed to benchmark assessment and poll results by age and gender. This information is used to understand patterns in the data and to support meaningful comparison across groups. It is not presented to The Day's administrative users alongside a student's direct identity.

Where information is linked to a username or account, we treat it as personal data where applicable under data protection law, even where the real-world identity is not visible to The Day administrators. We use pseudonymisation to reduce risk; pseudonymisation does not turn personal data into anonymous data.

How student data is used

Student data is used for the purposes agreed with the school or college and set out in the applicable DPA and service documentation. This includes providing and supporting the service, maintaining and improving the product, understanding how students use the platform and evaluating the impact of our work.

Assessment and poll data may be analysed in aggregated or pseudonymised form to identify patterns, benchmark results and contribute to our impact and evaluation work. We do not use student data to make decisions about individual students, and we do not use identifiable student information for advertising or direct marketing.

We will not use or disclose student personal data for a new purpose that is incompatible with the agreed processing arrangements. Where our planned use of data changes materially, we will review the legal, contractual, privacy and safe

Safeguarding

The safety and wellbeing of children and young people is central to how we design and operate our services. The school or college remains responsible for its own safeguarding arrangements and for responding to concerns about individual students in accordance with its safeguarding procedures.

The Day supports this responsibility through appropriate platform controls, role-based access, moderation processes and clear reporting routes. Where a concern is raised with The Day that may relate to the safety

or wellbeing of a child or young person, it will be handled in line with our Safeguarding Policy and escalated to the appropriate school or college contact or other authority where necessary and lawful.

Access by school or college staff

School and college administrators are responsible for managing user accounts and assigning access to authorised staff. Schools and colleges should promptly remove access when a staff member leaves, changes role or no longer needs access.

Teachers and administrators should only access student information for legitimate educational, safeguarding or administrative purposes. They must keep their login details secure and must not share accounts or access information that they do not need for their role.

Data retention and deletion

Student information is retained only for as long as it is needed for the agreed service and associated legal, contractual or operational requirements. Deletion and retention arrangements are managed in accordance with the applicable The Day data-retention procedures.

Where a school or college requests deletion or when a service ends, The Day will follow the agreed process for returning or securely deleting personal data, subject to any legal or contractual requirement to retain information.

Security incidents and concerns

If a school or college believes that student information has been accessed, disclosed, lost or used inappropriately, it should contact The Day promptly using the agreed support or data-protection contact. Early reporting helps us investigate and take action quickly.

The Day maintains a Data Breach Procedure for incidents involving personal data and will work with the school or college on notifications and remediation where required by law or contract.

Third-party suppliers

Where we use third-party technology providers to deliver the service, we select and manage them in line with our information-security and data-protection requirements. Appropriate contractual protections are used where a supplier processes personal data on our behalf.

The Day's key hosting environment for student data is AWS. Other service providers may support authentication, communications, monitoring or other functions. The specific processors and processing arrangements that apply to a school or college are governed by the relevant DPA and supporting documentation.

Responsibilities

The Day is responsible for maintaining proportionate information-security and safeguarding controls for the services it provides. Schools and colleges are responsible for appropriate use of the service, accurate user administration, safeguarding arrangements within their organisation and ensuring that only authorised staff have access.

Both organisations share responsibility for protecting student information. Good security depends on the practical actions of everyone who uses or supports the service.

Review

This policy will be reviewed at least annually and sooner where there is a significant change to our services, technology, security arrangements, legal or regulatory requirements, or the way student information is processed.