Description of service

Report + Support is a cloud-based online reporting tool which allows people to report any form of harassment, abuse or wellbeing issue they have experienced or witnessed to the organisation in a secure way. A trusted, secure solution for the safety of your people, the site also contains advice articles enabling users to seek support for what they have experienced or witnessed. It can be accessed 24/7/365.

Selected staff from the organisation are able to log into the administrative part of the tool to review the data entered by users. These will be in the form of incident reports and raw data. Incident reports are formatted for easy reading on screen. The data can be exported in a password protected Excel file for analysis outside the tool. This admin area of the site allows the organisation to interrogate the information submitted to the system, giving them the ability to monitor any themes or trends and report to stakeholders within the organisation. Those reporting anonymously will provide useful data to help spot trends and guide the organisation on what preventative action it might take.

The product is built and licensed by Culture Shift, and hosted by Amazon Web Services (hereafter referred to as AWS) across multiple availability zones for resilience

Backup and disaster recovery

Data is backed-up and securely stored off-site using a different AWS region from our main server hosting. The backup files are encrypted using AWS's best practice configurations.

We maintain a robust backup and recovery process that minimises the risks and operational impact to Culture Shift and its clients from service interruptions and potential loss of data integrity. We have a disaster recovery plan in place with detailed steps to recover systems and data depending on the scenario. We test this plan yearly to ensure it is fit-for-purpose.

Onboarding support

The whole process from contract commencement to your Report + Support site going live can take as little as 4-8 weeks. This time is divided between Key Meetings, Required Actions and Technical Requirements. Here is a summary of these steps:

Key Meetings

Welcome Meeting with your key contacts from the Culture Shift Success Team: Prior to this, the Culture Shift team will have created your Report + Support site with our Leading Practice Questions as default, and will provide the link to the organisation's team ready for review. During this time we will also agree on a 'go-live' date for your system.

Kick-Off Meeting: The wider project team are in attendance, and Culture Shift will discuss the Required Actions and Technical Requirements to go live (1 hour)

Dashboard Training: The software is intuitive and easy to use, so after this training the team will be able to complete the vast majority of customisation themselves.

Weekly touchpoint with your key Culture Shift contact: A regular catch-up to monitor progress.

Required Actions

Review reporting questions: The Culture Shift team will configure the reporting routes based on the information submitted. We will give you feedback on the questions based on our years of experience in creating Leading Practice reporting forms, and we will flag to you if there appears to be an amendment that we think would deter people from speaking up. All amendments can be reviewed in advance of the site going live.

Review support articles: The Culture Shift team can provide recommendations and share examples for these.

Complete privacy notice

Provide logo and branding for the reporting site

Confirm dashboard users and teams

Technical Requirements

Confirm dashboard access preference (SSO/MFA)

Configure DNS settings

Off-boarding

We have a robust, fully documented off-boarding process which ensures smooth transition away from the system. Some of the steps involved are:

Unpublish DNS settings

Export your data

Site deletion

Service levels

For information about performance, availability, maintenance and support hours, please refer to our service level agreement.

Technical requirements

For a Report + Support site to go live, under normal circumstances, it lives as a subdomain of your organisation. To do this, you must set up a CNAME DNS record to point the subdomain you want (this is usually reportandsupport.yourcompany.com) to an address which we will provide you.

We also use Amazon Certificates to manage security certificates for your domain. This requires a second CNAME to be created, which includes a randomly generated subdomain of your main Report + Support deployment.

Your Culture Shift contact will give you these details once your site has been set up. In advance of DNS being set up, you will be able to access your site via a randomly-generated URL to verify the setup.

Supported Browsers

The Report + Support product is built as a web application, and as such requires a modern web browser. For the administration interface, web browser versions with greater than 0.2% of global usage are supported on a best effort basis. No support guarantee is made for a web browser which does not meet this requirement.

The administration interface and public site are tested with the following browsers to verify this:

- Google Chrome on Windows and macOS (latest version only)
- Safari on iOS and macOS (latest version only)
- Edge (latest version only)

Outage and maintenance management

Report + Support is architected in such a way to be able to survive an outage of a single data-centre (AWS Availability Zone) in order to achieve a high level of service availability. In the event of an outage, your Customer Success Manager will contact your nominated lead by email to inform them of the outage and keep them up-to-date.

For further information please refer to our service level agreement.

Access to data

As a Culture Shift partner, you get to choose which of your staff and teams have access to reports and data. Our system enables you to customise different permissions and access rights for different teams, enabling security and confidence that the right people will see the relevant reports.

All data from your system can be exported in a password protected file. We encourage all partners to ensure the data downloaded is anonymised to reduce any risk of breach to data protection legislation.

No Culture Shift employee has access to your database containing report information. If access was needed, this would be coordinated with your organisation on a case-by-case basis. Culture Shift staff receive training on data protection and privacy compliance, and have access to independent experts when required.

We take compliance with the GDPR very seriously. Our platform is informed by advice from independent experts and the Information Commissioner's Office (ICO).

Personal Data is gathered by the system to help organisations determine the rates of harassment, abuse and assault within the organisation on the ground of Legitimate Interest.

You are responsible for ensuring data is retained in line with your own retention policy. The Culture Shift platform enables data redaction which allows for reports to be archived indefinitely.

Culture Shift uses 3 sub-processors to provide our service to you: Amazon Web Services, Mixpanel, and Sentry. In all of these cases these companies act as sub-processors and do not have any direct access to personal data, and the reports themselves are only stored within an Amazon Web Services database, with Mixpanel and Sentry only handling the names and email addresses of administrators and caseworkers. All of these sub-processors are either based in the EU, or we have standard contractual clauses in place to ensure compliance with the GDPR.

Security

We understand that when it comes to processing data from or relating to the people in your organisation, you can't take any risks. That's why we have gone beyond the legal requirements and regulations to provide the most secure reporting system available to our partners and the people they represent.

This means you can implement Report + Support with the confidence of knowing

all collected data is securely stored and managed. It also means that you can give the people in your organisation the same assurances ahead of them making a report.

We are accredited with Cyber Essentials and ISO27001 and have completely isolated our office network from the reporting site network to minimise the risk to any customer data.

The application uses a Serverless architecture combined with AWS CloudFormation, meaning that developers need no direct access to the infrastructure running the application. This makes management completely automated and auditable, and in the most part, directly managed by AWS. Developers have no direct access to the database, all direct changes made must be made through deploying code, which is audited and reviewed before being permitted to run.

By using the Serverless architecture, and making use of Amazon Virtual Private Cloud networking, we eliminate the risk of vulnerabilities and out-of-date software in the OS and networking level. You can find out more about Amazon's security policies on their website.

Our development practice is structured around a continuous delivery pipeline. To manage vulnerabilities and out-of-date patches in the application, automated scanning tools provided by the Node Security Project are used in this pipeline. These scans run regularly on each change made to the application, and any vulnerabilities are immediately flagged to the developer who must resolve them before they can make any further feature changes. Each change must also be manually reviewed by another developer before being accepted in the mainline, and automated tests are used to check for regressions, with new features and especially security critical code paths having additional tests written to cover them.

All public-facing services use HTTPS configured with the "modern" TLS cipher suite, meeting current industry standards for encryption. Inter-component encryption also uses HTTPS communication with the same configuration backed by AWS IAM roles and further locked down by AWS security groups, which are both configured with a "deny-by-default" policy and a whitelist of only permitted services. Database connections also use TLS 1.2 encryption in "verify full" mode, which is the strongest level supported by the AWS RDS database.

All data stored is also encrypted at rest using AES-256 following Amazon's best practice for doing so. The only exception to this is uploaded images that are used on the public-facing website in support articles and for branding, which are not encrypted.

Amazon web application firewalls and CDNs are used to protect against denial of service attacks as well as the application and database.

Amazon Cognito Advanced Security is applied to the log-in flow to protect

against brute-force attempts to log in to a user's account. For more information on this, please see Amazon's product documentation. We encourage all users to set up two-factor authentication using a TOTP-compatible authenticator app. Alternatively, an organisation can choose to use their single-sign on system, in which case any additional brute-force protection is delegated to that system.

The Culture Shift Platform is penetration tested annually to maintain confidence in the application.