GDPR - STATEMENT OF POLICY

17 May 2018

Introduction

The new EU General Data Protection Regulation (GDPR) comes into force on 25 May 2018 and will impact every organisation which holds or processes personal data. It will introduce new responsibilities, including the need to demonstrate compliance, more stringent enforcement and substantially increased penalties than the current Data Protection Act (DPA).

GDPR replaces the existing data protection regimes in place throughout the European Union (EU), including the UK, and introduces a number of new obligations and requirements on data controllers and processors.

Compliance

sQuid are fully aware of the requirements of the General Data Protection Regulations (GDPR) which will become effective on 25 May 2018. sQuid will be fully compliant and a statement of sQuid's policy follows.

Under GDPR the school is the data controller and sQuid, as a supplier, is the data processor. To deliver the sQuid solution some data is required to enable users to create logins and access the system. As a minimum, the forename and surname of the child, the Year and Class and a unique personal number.

There are 2 situations where sQuid need to use personal data in order for the software to deliver the full benefits.

Firstly, sQuid's online payment system that integrates with cashless catering software and/or secondarily, sQuid SchoolPay software.

For Catering, sQuid only need personal data that identifies the child at the point of serving. Typically, the forename and surname of the child, the Year and Class and a unique personal number. Although to ease the school's communication with parents, through letters, SMS or email, sQuid can also pull through Parental Information such as name and address, phone number, email address, and certain Student Groups used by the school.

For sQuid SchoolPay, the software enables schools to request and receive payment online for other activities (trips and offers). As this software includes a communication module (email/SMS messaging) we require: the forename and surname of the child, the Year and Class, a unique personal number and Parental Information such as name and address, phone number, email address and certain Student Groups used by the school.

Data Sharing Agreement

It should be noted that when a school agrees to use either of the above solutions that sQuid require a “Data Sharing Agreement” to be completed by the school, which details the exact data that the school agrees should be pulled from their MIS before any installation work is started. In each instance that a school proceeds in signing the Data Sharing Agreement, the school is thereafter in control and responsible for managing, maintaining, updating and accessing all data in sQuid.

Data Processing

Data will be processed fairly and lawfully, only processed for specific purposes and when the correct form of consent has been obtained. sQuid will ensure that all the data that we process is accurate; where necessary kept up to date; and only processed in accordance with an individual’s rights.

Data Storage

All data held by sQuid is securely stored in a fortified remote data centre within the EU. Data is monitored 24/7/365 and all servers are backed up to a central tape system at a tier 1 hosting provider with 28 day retention. The cycle is daily incremental with a weekly full backup that is taken offsite and stored in a highly secure, purpose built building. A full audit trail of any data movement can be produced upon request.

Data Security

We recognise that we are legally obliged to use information in line with all current, and future laws concerning the protection of personal information; including the General Data Protection Regulation effective 25 May 2018, the Data Protection Act 1998 (these laws are referred to collectively in our Privacy Policy as the "data protection laws” see https://www.squidcard.com/privacy-policy for the detail of our policy.)

sQuid is registered with the Information Commissioners Office (ICO). Our registration number is Z1327001.

Summary

1. We are committed to ensuring that your personal information is secure. In order to prevent unauthorised access or disclosure we store personal data in a fortified remote data centre protected by dual firewalls using the latest technology. That data is backed up on a nightly basis and held off site in a separate data centre.
2. Personal information is minimised before being securely transmitted and is password protected at all times.
3. Stored payment card details are encrypted to meet PCI DSS standards.
4. The whole infrastructure is monitored 24/7/365 through automatic checking of the services operating both from a systems and business application perspective. There are strict SLA’s in place.
5. Transactions that take place at a local point cannot fail as each event is stored securely in the back office and the information will be synchronised with the payment engine as soon as normal service is resumed. Each event has a unique sequence number that is securely communicated between the terminal/till and host, which ensures that no transaction data is either misplaced or duplicated.

If there are further questions, please email dataprotection@squidcard.com

Or alternatively, for more information on GDPR legislation, please visit the Information Commissioner's Office website at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr