# GDPR - STATEMENT OF POLICY

**17 February 2021**

## Introduction

On January 1st 2021 the United Kingdom formally and effectively left the European Union.

In anticipation of the UK withdrawing from the EU UK data privacy laws were amended, the amendments are all contained in the UK government's *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019*, also known as the DPPEC regulations.

DPPEC regulations took effect on January 31st, 2020 in accordance with the UK governments EU Withdrawal Agreement.

The DPPEC regulations do two major things:

1. create a "new" domestic law known as UK-GDPR.
2. revise the Data Protection Act 2018.

The revisions to the Data Protection Act 2018 are also effective from January 31st, 2020.

## Compliance

sQuid's business policy is to ensure that it is fully aware of the requirements of the UK General Data Protection Regulations (UK-GDPR) and to be compliant. Because of the nature of our networking business, where data is shared in certain situations, we need to work with our Partners to ensure the entire 'system' is compliant.

Under UK-GDPR, a contracted Partner is typically the **Data Controller** and sQuid is the **Data Processor**. To deliver the contracted service to end customers, sQuid is required to use some data collected by a Partner to facilitate the creation of online eMoney (and other digital) User Accounts along with the creation of and payment for online transfer requests made by system users.

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's Trips & Offers 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 Trips & Offers**, 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.

# GDPR - STATEMENT OF POLICY

## 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 by sQuid

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

## Data Storage

All data held by sQuid is stored in a secure, fortified remote data centre operating within the UK. Services (and thus the 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 secure data store building. A full audit trail of any data movement can be produced upon request, and our systems have full logging.

## Data Security

sQuid is legally obliged to use information in line with all current, and future laws concerning the protection of personal information; including the UK General Data Protection Regulation, the Data Protection Act 2018 both effective from January 31st 2020 (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.

# GDPR - STATEMENT OF POLICY

## Summary


1. We are committed to ensuring that 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, and we use tokenised systems for processing payments from end customers.
4. Our systems infrastructure is monitored 24/7/365 through automated checking processes that manage hardware, operating software and business applications. We maintain Service Level Agreements and operate according to these.
5. Transaction events in the sQuid network that take place at a local point are stored securely in the back office and then synchronised with the central processing engine (this allows for a local failure in connectivity, without loss of data). Each event has a unique sequence number that is securely communicated between the local transaction location and the central host, which ensures that all transaction data is uniquely identified and thus tracked through the system.


For further information, please contact us by email **dataprotection@squidcard.com**

For more information on GDPR legislation, please visit the Information Commissioner's Office website at: **Data**