Dear Data Processing Officer

GDPR

European data protection was significantly revised with the adoption of the General Data Protection Regulation (GDPR) in May 2018. Cauliflower Group Ltd is committed to meeting its obligations and conducts regular GDPR reviews to ensure compliance with these additional rules. This has been integrated with our current Data Protection Procedures and we will continue to review and update our procedures with any Company changes and developments. We are registered with ICO and have declared the information we hold.

Overview of the key GDPR areas that we annually review are as follows:

- **Audit:** We audit the data we have and its storage, access and security.
- **Privacy by design:** Under ICO guidance we currently only collect information from customers that is succinct and relevant for processing jobs. Under GDPR we review our security of this information both through internal security and web hosting services.
- **Governance and Accountability**: At management level we review and updated policies & procedures to safeguard data and demonstrate compliance. This includes data mapping and privacy impact assessments where relevant.
- **Raising awareness:** Induction and further training opportunities for our staff ensure that we raise their awareness of data protection and company policy.
- **Consents, notices and contracts**: We review these to ensure they are updated to reflect legal requirements.
- **Transfers:** We no longer transfer to data entry companies all data is kept inhouse.
- **Incident response**: We regularly review our policy and processes to ensure we are ready for requirements with regard notify authorities and users of data breaches in certain circumstance as specified by law.
- **Lawful Basis for Processing Data in our Marketing:** We are continuing to ensure that we market to individuals who have a 'legitimate interest' (as previous customer) in the products we offer and that they are offered an opt out from further contacts of legacy communications and opt ins for ongoing new communications.

Our data protection policy contains a full AUDIT of the data we collect and how it is handled.

Cauliflower Group Ltd

DATA PROTECTION POLICY

Compliance with the Data Protection Act 1998

Principle 1: Processing personal data fairly and lawfully

• Cauliflower Group will only use the data provided by the customer in a way that they would reasonably expect to produce their order.

• No personal data is passed on to third party companies.

Principle 2: Processing personal data for specified purposes

Cauliflower Group will only obtain customer's personal data for the purpose of their order and that data shall not be further processed in any manner incompatible with that purpose.

Principle 3: Holding personal data that is adequate, relevant and not excessive

Cauliflower Group will only hold personal data about an individual that is sufficient to produce their order and future reorders.

Principle 4: Personal data shall be accurate and, where necessary, kept up to date

Cauliflower Group updates their customer database continuously - contact details are removed, updated and/or replaced.

Principle 5: Duration we hold Personal Data

Cauliflower Group only holds a modest amount of personal data. They conduct an annual audit on each registration renewal to check through the records they hold to make sure they are not holding onto personal data for longer than is required.

Users of Cauliflower Groups Online Creators can at any point permanently delete all data they have entered in the system.

Cauliflower Group will delete all personal data on any inactive accounts after a rolling period of 18 months. This will remove all personal, bespoke and order information from your account.

Principle 6: Personal Data and the Right to Opt Out

Cauliflower Group includes a tick box on Pupil Order Forms where a customer can request the submitted artwork is not used for future samples. Any referral to a customer is deleted from any images used for promotional or advertising purposes.

Cauliflower Group only contact individuals by email when their details have been obtained in the course of a sale and only contacts them about similar products and services they provide. The individual is given the opportunity to opt out of receiving further marketing messages.

Principle 7: Security to prevent the personal data held being accidentally or deliberately compromised.

Premises Security

• Cauliflower Group has secure alarmed premises attached to a Red Care Monitoring station.

• The Premises has front and rear building CCTV.

Courier Services

Use of Nationally recognised courier service that has received government contracts with schools in the past - including KS2 exam paper collection/deliveries.

Third Party Enquiries

• All staff to be aware of Data Protection.

• All staff are trained in the company security measures including:

• To be wary of people who may trick them into giving out personal details.

• Not to send offensive emails about other people, their private lives or anything else that could bring the Company into disrepute.

• Not to believe emails which appear to come from the bank asking for credit cards details or a password.

• Not to open spam.

• Reorders of Books will only be processed when placed through the child's school or original customer.

• Reorder of School Cards can only be made using the child's unique code.

Computer Security

Internal computers:

• Have Microsoft Security Essential virus checking software loaded, and are set up to receive the latest patches and security updates.

• Incoming emails are delivered by a large email supplier 123.Reg and are scanned by Net Intelligence.

• Computers are scheduled to connect to the internet during office hours only and time out after a 20min period.
• Staff only have access to the information they need to do their job and do not share passwords.
• Regular backups are taken so information is not lost.
• All personal information is removed before disposing of old computers.

Web and Online Service Hosting Security

This is outsourced to a large well established company: Amazon EC2 Webservices:
As the biggest web services supplier it complies with all Physical Security and Data Transfer requirements. This is hosted in Ireland - part of the EEC.
Amazon is certified under ISO 27001:2013 (expiry of current certificate 11/07/2019. Please visit AWS for their Compliance details: **https://aws.amazon.com/security/**

Site Online Security

• Each online user for our online creator systems must register their details to receive a unique password.
• Our School User Passwords are set to different security levels which allow for a range of access to data - this is control by the organiser of an online project.
• Time settings can be controlled by a School Project Organiser to allow younger users who have passwords limited access to Cauliflower Group book Creator site. (ie school hours only)
• SSL certificates are in place for all data transfer requirements.

Printed Information

• All confidential paper based data is archived on site for a period of 12 months.
• The company then shred all sensitive material including order forms, cards and yearbooks before disposing of materials.

Online Transactions

• These are made directly through Stripe. This company complies with processing procedures for Online Payment Requirements.
• We do not record or store any bank card details or take over the phone payments.

Below please find the data we will hold with regard school orders:

Customer Information Audit

- Xero Accounts Software - Invoice Details
- Cauliflower Data Base - Customer Contact Details
- Print Files used for production
- Physical Products Manufactured (before shipping)
- Data Transfers - Data entry temps or outsourced
- Online Orders details made from our Websites - (Cleared after each project)
- Emails - (cleared on regular periods)
- Accountants - holds copy of sales information and accounts set up with us
- Parents Hard Copy Order Forms (returned to schools)
- Parcel Force Database - Customer name and address

Data processed and held for each order

Online Orders

Orders are placed online by parents

Childs Name/Nick Name (as required by parent on printed product)	Entered by Parent online - stored on our database
Quantity Order information - provided by parent	Entered by Parent online - stored on our database can be deleted by parent
Class Name	Entered by parent and changed to a LETTER by our software
Delivery Address - for reorders	Entered by parent online - stored on our database and can be deleted by parent
Accounts with unique login details and password are created. Pupils are identified by a unique code printed on their order form - the unique code identifies all files associated with the order.	

Name of Organiser - with contact details	Entered online by school organiser and held on company database
Delivery address of Organisation	Entered online by school organiser and held on our company database
School identification codes	Enter by office staff and held on our company database

Protecting Identity:

- There are processes in place to allow individual pupils within a school, in sensitive situations to participate in our projects without names /school logos/ being associated with products if the rest of the school wish to include these features.

- School Name, Childs Name and School Logo are an optional identifying feature which schools may choose to include if they wish - this does not form a requirement for any of our projects.