Description of Security Measures Employed to Safeguard the Processing of Personal Data

1. Organisational

a. Policies & Documented Procedures

Policies relating to information governance issues are drafted by employees with detailed knowledge of legal requirements and the Organisation's processes. All policies have documented review dates and ownership is assigned. Reviews are held ahead of the expiry date or sooner where there is an identified issue. All policies follow a governance route for approval. Key policies are published to the organisation's website for transparency.

b. Roles

The organisation has a named Data Protection Officer who is Paul Turner. This Officer executes the role by reporting the outcome of statutory processes to Margaret Lee who acts as the organisation's Senior Information Risk Owner.

c. Training

The organisation regularly reviews our employee roles to ensure that training and awareness messages are appropriate to the nature and sensitivity of the data processing undertaken. Induction processes ensure new employees receive appropriate training before accessing personal data, and all other employees receive refresher training annually. All training received is documented for evidence purposes.

d. Risk Management & Privacy by Design

The organisation identifies information compliance risks on its risk register. Risks are assigned clear ownership, rated against a consistent schema, appropriate mitigations are identified and are annually reviewed.

e. Contractual Controls

All Data Processors handling personal data on behalf of the organisations have given assurances about the compliance of their processes; either through procurement assurances/ evidence, contractual agreement controls, risk assessments or supplementary statements.

f. Physical Security

All employees or contractors who have access to our premises where personal data is processed are provided with Identity Cards which validate their entitlement to access. The organisation operates processes which ensure only those individuals who have an entitlement to access premises are able to. Access to physical storage holding sensitive personal data is further restricted either through lockable equipment with key or code control procedures or through auditable access to specific rooms/ areas of buildings.

g. Security Incident Management

The organisation maintains a security incident process which, with the support of appropriate training, defines what constitutes a breach of these security measures to facilitate reporting of incidents. The process covers investigation of incidents, risk rating and decisions over whether to notify an incident to the Information Commissioner's Office (ICO) within the statutory timescale. Incidents are reported to senior leaders and actions are consistently taken and lessons learned implemented.

2. Technical

a. Data at Rest

i. Use of Hosting Services

Some personal data is processed externally to the organisation's managed environment by third parties in data centres under agreed terms and conditions which evidence appropriate security measures.

EES for Schools uses Business Catalyst (Adobe) as a website platform. Business Catalyst's data centres are hosted by Amazon Web Services in the United States of America, Australia and the United Kingdom. Data is secured by Amazon's technologies including AWS Identity and Access Management, AWS Certificate Manager, AWS CloudHSM, Amazon GuardDuty and Amazon Inspector.

EES for Schools' uses dotmailer as its email marketing software. The core dotmailer platform is hosted on high security Microsoft Azure data centres. Data for European clients is held in the West Europe region, with data being backed up to the North Europe region. All Azure facilities meet a broad set of compliance standards. In addition to our virtualised infrastructure hosted on

Azure, dotmailer has a physical data centre located in London. This connects to Azure via a Virtual Private Network, and is used to send Client email campaigns out to the internet. This holds various accreditations including ISO 27001 & 22301.

Target Tracker is hosted on Essex County Council’s Azure Tenancy at data centres in the European Economic Area.

ii. Firewalls

Access to the organisation’s managed environment is protected by maintained firewalls. Business needs to provide access through the firewall go through a strictly documented change control process which include risk assessment and approval.

Dotmailer deploys firewalls at network perimeters; running management authorised rule sets.

iii. Administrator Rights

Enhanced privileges associated with administrator accounts are strictly managed. Administrator activities are logged and auditable to ensure activity can be effectively monitored.

iv. Access Controls

Access permissions to personal data held on IT systems is managed through role based permissions authorised by managers. Managers of appropriate seniority inform administrators of additions, amendments and discontinuation of individual accounts within permission groups. Managers are periodically required to confirm that current permissions for which they are the authoriser and employees associated with these permissions are accurate.
Dotmailer employs a dedicated privacy & compliance team (with a nominated Data Protection Officer) to oversee the security, privacy and compliance programmes of the organisation. Dotmailer restrict access to workspaces, and secure data centre facilities were information systems that process personal data are located to identified authorised individuals.

v. Password Management

The organisation and systems used by EES require a mandatory password complexity combination of minimum length and characters, and regular enforced password changes.

vi. Anti-Malware & Patching

The organisation has a documented change control process which facilitates the prompt implementation of any security updates provided by the suppliers of active software products.

Dotmailer’s maintenance schedule facilitates timely installation of security patches as well as installing and regularly updating anti-virus software.

vii. Disaster Recovery & Business Continuity

As part of the organisation’s business continuity plan, there is provision to ensure effective processes are in place to both safeguard personal data during a service outage incident and to re-establish secure access to the data to support data subject rights in ongoing service provision.

The Dotmailer platform is built using redundancy and load balancing at every level reducing service disruption due to single component failure. Data on the system is backed up and will resume at a secondary facility in case of a catastrophic event.

b. Data in Transit

i. Secure email

The organisation has access to secure email software for communicating with some third parties where licensing agreements permit this. Sensitive data will be sent using such tools where available. Where software is not available a system of password protecting sensitive data in email attachments is employed.

ii. Secure Websites

The organisation maintains a website which allows for secure transfer and access to personal data through account credentials across a virtual private network. The website security measures are managed by Business Catalyst (Adobe) and Amazon Web Services as service providers.

iii. Encrypted Hardware

Devices which store or provide access to personal data (such as laptops) are secured by password access with ‘remote wipe’ safeguards for reported device loss or theft. Removable media such as memory sticks can be read by laptops and desktops but data cannot be added to removable media without the device being encrypted.

iv. Hard-Copy Data

The removal of personal data in hard-copy form is controlled by organisational policy which requires employees to take steps to conceal the data and appropriately secure the data during transport.

These security measures are reviewed annually and approved as accurate and appropriate by the organisation’s governance process.