Data Protection Policy

1. Introduction

Project Q (trading as ac3 solutions limited) supports and adheres to the GDPR as required by law. This policy provides further clarity to the key aspects and the roles of the Data Processor (Project Q) and of the Data Controller (School) in their responsibilities in upholding the core principles.

1.1 Background to the General Data Protection Regulation ('GDPR')

The purpose of the General Data Protection Regulation April 2016 is to protect the fundamental rights and freedoms of persons and their right to the protection of personal data. It lays down rules for the protection and processing of personal data.

1.2 Definitions drawn from the GDPR for the purpose of this policy:

Child: GDPR defines a child as anyone under the age of 16. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Consent: of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Controller (data): the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject: any living individual who is the subject of personal data held by an organisation.

Personal data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach**:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Profiling**:** any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Recipient: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

Third party: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

2. Responsibilities and Roles

2.1 The school is the Data Controller under GDPR. Management of school are responsible for developing and encouraging good information handling practices within school and we would expect that the Data Protection Officer (DPO), a role specified in the GDPR, is accountable for the management of personal data and for ensuring that compliance with data protection legislation and good practice can be demonstrated.

2.2 Project Q is the Data Processor under GDPR. The management of Project Q, located at Lockside Office Park, Preston, PR2 2YS, are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Project Q collects and processes in accordance with the General Data Protection Regulation (GDPR).

2.3 The GDPR and this policy apply to all of Project Q personal data processing functions, including those performed on clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

2.4 The Data Protection Officer is responsible for reviewing the register of processing annually in the light of any changes to Project Q activities and to any additional requirements identified by means of data protection impact assessments.

2.5 This policy applies to all Employees/Staff and interested parties of Project Q such as outsourced suppliers. Any breach of the GDPR will be dealt with under Project Q disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

2.6 Partners and any third parties working with or for Project Q, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by Project Q without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which Project Q is committed, and which gives Project Q the right to audit compliance with the agreement.

3. Data Protection Principles – Project Q as the 'Data Processor'

Project Q is a Data Processor acting on behalf of the 'Data Controller' (school).

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Project Q's policies and procedures are designed to ensure compliance with the principles.

As a Data Processor, Project Q will adhere to the following principles:

3.1 The Processor must have adequate information security in place

- Staff are provided with training and are contractually required to adhere to the GDPR policy
- All staff are DBS checked
- Access to data is carefully managed and restricted and only on request from a Data Controller. Access is audited
- Our Data Centre is a UK based, owned, approved Government Procurement Service provider. Our Servers are dedicated and managed by our internal team.

- Our servers and services are protected by a robust backup and mirroring system. Regular snapshots are routinely and securely transferred from our national data centre to our head offices forming part of our disaster recovery solution
- Strong password protection with automatic locking of idle computers and servers
- All computers and servers are routinely patched and are protected by antivirus, antimalware, soft and hardware-based firewalls along with a DDOS protection system

3.2 The Processor must not use sub Processors without consent of the Controller

Project Q does not employ sub processors or third-party contractors. Project Q requires the use of infrastructure suppliers such as telecommunication and email service providers in order to send text messages and emails these are governed by contracts and adhere to the GDPR.

3.3 The Processor must cooperate with the relevant Data Protection Authorities in the event of an enquiry

If contacted, Project Q will collaborate with the Information Commissioner's Office and inform the Data Controller if there is a related request.

3.4 The Processor must report data breaches to the Controller without delay

Project Q will react immediately and appropriately of a data breach including isolation of services and forensic resolution. This will be reported to the Data Controller as soon as possible and be completed with full transparency.

3.5 The Processor has a named Data Protection Officer

The Data Protection Officer is Alan Cree (Managing Director)

3.6 The Processor must keep records of all processing activities

Project Q is transparent, and all processing is evident through the Project Q Portal. The Data Controller can view all data directly from the secure portal. Project Q has established a data inventory and data flow process as part of its approach to mitigating risk.

3.7 The Processor must comply with EU trans-border data transfer rules

Data is not transferred outside of the UK

3.8 The Processor must help the Controller to comply with data subjects' rights

It is the Data Controller's responsibility to respond to a Subject Access Request. Project Q will support the Data Controller in the event of a request but will not liaise directly with a Data Subject.

3.9 The Processor must assist the Data Controller in managing the consequences of data breaches

Project Q will react immediately and appropriately in supporting a data breach by the Data Controller.

3.10 The Processor must delete or return all personal data at the end of the contract at the choice of the Controller

At the end of a contract, Project Q will erase the data from the Project Q system.

3.11 The Processor must inform the Controller if the processing instructions infringe GDPR

Project Q will inform the Data Controller if a request for processing infringes upon the GDPR.

4 Data Protection Principles – 'School' as the Data Controller

We require schools as Data Controllers to adhere to the 7 key principles as defined by GDPR and set out by the Information Commissioner's Office.

4.1 (1) Personal data must be processed lawfully, fairly and transparently

The Data Controller must identify valid grounds under the GDPR (known as a 'lawful basis') for collecting and using personal data.

The Data Controller must ensure that processing data is not in breach of any other laws.

The Data Controller must use personal data in a way that is fair. This means the Data Controller must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.

The Data Controller must be clear, open and honest with people from the start about how personal data will be used.

4.2 (2) Personal data can only be collected for specific, explicit and legitimate purposes

The Data Controller must be clear about what your purposes for processing are from the start.

The Data Controller needs to record your purposes as part of the documentation obligations and specify them in the privacy information for individuals.

The Data Controller may only use personal data for a new purpose if either it is compatible with the original purpose, or consent is obtained, or have a clear basis in law.

4.3 (3) Personal data must be adequate, relevant and limited to what is necessary for processing

The Data Controller must ensure the personal data to be processed is:

- Adequate and is enough to properly fulfil the stated purpose
- Relevant and has a rational link to that purpose
- Limited to what is necessary and do not hold more than is needed for that purpose.

4.4 (4) Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

The Data Controller should take all reasonable steps to ensure the personal data held is not incorrect or misleading as to any matter of fact.

The Data Controller may need to keep the personal data updated.

If the Data Controller discovers that personal data is incorrect or misleading, it must take reasonable steps to correct or erase it as soon as possible.

The Data Controller must carefully consider any challenges to the accuracy of personal data.

4.5 (5) Personal data must be kept in a form such that the data subject can be identified only as long as is necessary

The Data Controller should ensure that policies and routines are in place to ensure

- Personal data is not kept for longer than needed
- Retention periods are adhered too to comply with documentation requirements
- Periodic review of the data held and erase or anonymise it when no longer needed
- Consideration if given to any challenges to the retention of data. Individuals have a right to erasure if data is no longer need.

4.6 (6) Personal data must be processed in a manner that ensures the appropriate security

The Data Controller must ensure that personal data is processed secured by means of 'appropriate technical and organisational measures'.

The Data Protection Officer should consider the following technical measures:

- Password protection
- Automatic locking of idle computers
- Removal of access rights for USB and other portable media
- Antivirus, Antimalware software and firewalls
- Role-based access rights including those assigned to temporary staff
- Encryption of devices that leave the organisations premises such as laptops
- Security of local and wide area networks

The Data Protection Officer should consider the following organisational measures:

- Appropriate staff training levels
- Inclusion of data protection in employment contracts
- Identification of disciplinary action measures for data breaches
- Monitoring of staff for compliance with relevant security standards
- Review of clear desk policy
- Managing the use of portable electronic devices outside of the workplace
- Manage the use of employee's own personal devices being used in the workplace
- Adopting clear rules about passwords
- Making regular backups of personal data and storing the media off-site

4.7 (7) The controller must be able to demonstrate compliance with accountability and governance

The Data Controller must be able to demonstrate compliance with the GDPR. Measures such as the following should be considered:

- Adopting and implementing data protection policies
- Taking a 'data protection by design and default' approach
- Putting written contracts in place with organisations that process personal data on your behalf
- Maintaining documentation of your processing activities
- Implementing appropriate security measures
- Recording and, where necessary, reporting personal data breaches
- Carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests
- Appointing a data protection officer and adhering to relevant codes of conduct and signing up to certification schemes

4.8 Individual (Data Subjects') rights

The Data Controller must uphold the following GDPR rights for individuals where applicable and be Aware that the 'right' is not absolute:

- The right to be informed
- The right of access (Subject Access Request)
- The right to rectification
- The right to erasure
- The right to data portability
- The right to object (use in direct marketing)
- Rights in relation to automated decision making and profiling

This policy was approved by A Cree, Managing Director of Project Q (trading as ac3 solutions limited) on 20th March 2019 and is issued on a version controlled basis.

Signature: Date:

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	A Cree	20.03.2019