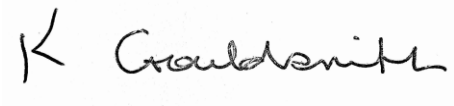
ACE Schools Multi Academy Trust

Data Protection by Design and by Default

Issue	Date	Author/Reviewer Job Role	Comments	Signed by DPO
	12/3/19	*Kristy Gouldsmith*		

Contents

Data protection by design and by default

1 GDPR Definition

1.0 Paragraphs 1&2, Article 25:

1.1 Para 1: Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

1.2 Para 2: The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

2 Considerations

2.0 ACE Schools MAT needs to ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. For example, when:

2.01 Building new IT systems for storing or accessing personal data;
2.02 Developing legislation, policy or strategies that have privacy implications;
2.03 Embarking on a data sharing initiative;
2.04 Using data for new purposes.

2.1 There are 6 foundational principles of Data Protection by Design:

2.1.1 Proactive controls not reactive;
2.1.2 Privacy as the default setting;
2.1.3 Privacy as a foundational requirement – not a bolt-on;
2.1.4 End-to-end privacy – Protection at all stages of the processing;
2.1.5 Visible and Transparent – easy for users to see and understand;
2.1.6 Part of the full functionality of the system.

2.2 The above considerations must be built into the Change Management and Change Review processes.