GDPR
SPECIAL CATEGORY DATA POLICY

Review Programme:	**March 2020**
Date for next review:	**March 2021**

Special category and criminal conviction personal data (the appropriate policy document)

Personal Data: means any information relating to an identifiable natural person, whether they can be directly or indirectly identified by reference to name, identification number, online identifier, or to specific things such as physical, physiological, genetic, mental, economic, cultural or social identity factors.

Special Category Data: This refers to very specific groups of personal data such as race or ethnic origin, political views, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for the purposes of identifying an individual, health and sexual orientation.

Criminal Conviction Data: This refers to criminal convictions and offences or related security measures including personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing.

This document meets the requirement at paragraph 1 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.

It also meets the requirement at paragraph 5 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The specific conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 to the Data Protection Act 2018 and the School intends to rely on these as and when appropriate, with particular reliance on paragraph 18, 'Safeguarding of children and individuals at risk'.

We process criminal offence data under Article 10 of the GDPR. Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations. We process criminal offence data for the following purposes; in parts 1 and 2 of Schedule 1, Paragraph 1, employment, social security and social protection and Paragraph 6(2)(a), statutory purposes. We notify individuals of the collection of criminal conviction data in the employee and recruitment application privacy notice.

Procedures for securing compliance

Article 5 of the General Data Protection Regulation sets out the data protection principles. These are our procedures for ensuring that we comply with them. These apply to all personal data processed by the School including special category data.

Principle 1

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The School will:

- ensure that personal data is only processed where a lawful basis applies, and where processing is otherwise lawful
- only process personal data fairly, and will ensure that data subjects are not misled about the purposes of any processing
- ensure that data subjects receive full privacy information so that any processing of personal data is transparent

Principle 2

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The School will:

- only collect personal data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a privacy notice
- not use personal data for purposes that are incompatible with the purposes for which it was collected. If we do use personal data for a new purpose that is compatible, we will inform the data subject first

Principle 3

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The School will only collect the minimum personal data that we need for the purpose for which it is collected. We will ensure that the data we collect is adequate and relevant.

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

The School will ensure that personal data is accurate, and kept up to date where necessary. We will take particular care to do this where our use of the personal data has a significant impact on individuals.

Principle 5

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

The School will only keep personal data in identifiable form as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. Once we no longer need personal data it shall be deleted or rendered permanently anonymous.

Principle 6

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The School will ensure that there appropriate organisational and technical measures in place to protect personal data.

Accountability principle

The controller shall be responsible for, and be able to demonstrate compliance with these principles. The governing body and Senior Leadership Team responsible for ensuring that the department is compliant with these principles in relation to the processing of personal data including special category data.

We will:

- ensure that records are kept of all personal data processing activities where appropriate, and that these are provided to the Information Commissioner on request
- carry out a Data Protection Impact Assessment for any high risk personal data processing, and consult the Information Commissioner if appropriate
- ensure that a Data Protection Officer is appointed to provide independent advice and monitoring of the departments' personal data handling, and that this person has access to report to the highest management level of the department
- have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law
- adopting and implementing data protection policies and ensuring we have written contracts with our data processors
- Implementing appropriate security measures in relation to the personal data we process

Data controller's policies as regards retention and erasure of personal data

We will ensure, where personal data including special category data is processed, that:

- there is a record of that processing, and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data
- where we no longer require special category or criminal convictions personal data for the purpose for which it was collected, we will delete it or render it permanently anonymous
- data subjects receive full privacy information about how their data will be handled, and that this will include the period for which the personal data will be stored.