Data Protection Policy
Trust Policy

Accountable Trust Committee	Audit & Risk
Policy Area	Risk
Responsible Officer	Commercial Director
Status	Published
Policy Rationale	Statutory
Categorisation	Trust wide
Implementation Date	1st October 2021
Publication	Internal
Review Cycle	Annual
Next Review Date	Autumn 2022
Related Documents	
Trust/school-mandatory policies	Freedom of Information Policy
Trust procedures and forms	Data Protection Policy Compliance Declaration Data Privacy Notice Data Processing Procedure Data Retention Procedure Record of Processing Activity Procedure Security Incident Procedure Surveillance Management Procedure Trust Service Request Database - Privacy Impact Assessment - Statutory Information Request - Security Incident - Policy Exception
Optional school policies	
External	ICO (ico.org.uk)

Document Control

Date	Version	Comments
01/10/21	1.0	Trustee approved – board meeting 29/09/21, with committee name update A&R
03/03/22	1.0a	Reference company name change to Learning Partners Academy Trust

Contents

1 Policy Statement 5
2 Legal framework 5
3 Roles and Responsibilities 5
3.1 Data Protection Officer 5
3.2 CEO/Headteacher 6
3.3 Trust Central Team 6
3.4 School Business Managers 6
3.5 All Staff (and related parties) 6
4 Data Protection Principles 7
4.1 Key Terms 7
4.2 Demonstration of Compliance 8
4.3 Core Principals 8
a) Processed lawfully, fairly and in a transparent manner 8
b) Collected for specified, explicit and legitimate purposes. 8
c) Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed. 9
d) Accurate and, where necessary, kept up-to-date 9
e) Kept for no longer than is necessary for the purposes for which it is processed 9
f) Processed in a way that ensures it is appropriately secure. 9
5 Data Protection Rights 9
5.1 The right to be informed 9
5.2 The right of access 10
5.3 The right to rectification 11
5.4 The right to erasure 12
5.5 The right to restrict processing 13
5.6 The right to data portability 13
5.7 The right to object 14
a) Processing for direct marketing purposes 14
b) Processing for research purposes 15
c) Objection Procedures 15
6 Education Data Processing 16
6.1 Safeguarding Information 16
6.2 Schoolwork 16
6.3 Examination data 16
6.4 Online Services for Children 16
6.5 CCTV 17
6.6 Photography and video footage 17
6.7 Biometric Data 18
a) Processing 18
b) Risk Review 18
c) Consent for Pupils 18
d) Consent for Adults 19
e) Non-participation 19
6.8 DBS data 20
7 Information Governance 21
7.1 Employee and related-party responsibilities 21
7.2 Line Manager responsibilities 21
7.3 Trustee responsibilities 21
8 Data Processing 22
8.1 Employee and related-party responsibilities 22
a) Daily processing activity 22
b) Advanced processing 23
8.2 Line Manager responsibilities 24
8.3 Central Team responsibilities 24

9 Acceptable Personal Use of Resources and Assets 26
9.1 Employee and related party responsibilities 26
a) Daily processing activities 26
b) General code of conduct 27
9.2 School Business Manager / Business Unit lead responsibilities 27
10 Data Handling Security 28
10.1 Employee and related-party responsibilities 28
a) Daily processing activity - onsite 28
b) Daily processing activity - offsite 29
10.2 School Business Manager responsibilities 31
10.3 IT Team responsibilities 32
11 Records Management (Retention) 33
11.1 Employee and related party responsibilities 33
a) Daily activity 33
b) Advanced processing 33
11.2 School Business Manager responsibilities 34
11.3 IT Network Team responsibilities 34
12 Statutory Requests for Information 35
12.1 Employee and related party responsibilities 35
12.2 SBMs or delegated request coordinator responsibilities 35
12.3 Central Team 37
13 Security Incidents 38
13.1 Employee and related party responsibilities 38
13.2 School Business Manager responsibilities 38
13.3 Headteacher/CEO responsibilities 39
13.4 Central Team 39
13.5 DPO responsibilities 40
14 Appendix 1: Lawful Processing 41
14.1 Generic Conditions 41
14.2 Sensitive Data Processing 41
14.3 Consent 42
14.4 Automated decision making and profiling 42

Key Contacts

Trust	01483-888188
Data Protection Officer	DPO@learningpartners.org
Commercial Director & Deputy DPO	ALFish@learningpartners.org
Head of IT	BSayers@learningpartners.org
Trust Data Privacy Notice	https://www.learningpartners.org/11/privacy-statement
Trust Service Request Database	https://www.learningpartners.org/959/service-request-database (For reporting potential breaches/data incidents)
Schools	
Boxgrove Primary School	01483-563701 SBM: IDickinson@boxgrove.surrey.sch.uk DP Contact: JSharp@boxgrove.surrey.sch.uk
Fullbrook School	01932-349301 SBM & DP Contact: TorranceP@fullbrook.surrey.sch.uk
George Abbot School	01483-888000 SBM: SJones@georgeabbot.surrey.co.uk DP contact: KOSullivan@georgeabbot.surrey.co.uk
Guildford County School	01483-504089 SBM & DP Contact: mcheesman@guidfordcounty.co.uk
Guildford Grove Primary	01483-504713 SBM & DP Contact: admin@guildfordgrove.surrey.sch.uk
Kings College, Guildford	01483-458956 SBM & DP Contact: P.Torrance@kingscollegeguildford.surrey.sch.uk
Loseley Fields Primary School	01483-416477 SBM & DP Contact: SBM@loseleyfields.surrey.sch.uk
Northmead Junior School	01483-529870 SBM & DP Contact: Deborah.Cole@northmead.surrey.sch.uk
Pirbright Village Primary School	01483-473884 SBM & DP Contact: HMuller@athenaschools.co.uk
Sandfield Primary School	01483-566586 DP Contact: Jane.Cregan@sandfield.surrey.sch.uk
Shalford Infant & Nursery School	01483-562143 SBM & DP Contact: Finance@shalford.surrey.sch.uk
Stoughton Infant School	01483-504172 SBM & DP Contact: SRalph@stoughton.surrey.sch.uk

Please note this list may be updated by the responsible officer when change arises in the organisation, without the need for committee meeting review/approval.

1 Policy Statement

The Board of Directors of Learning Partners Academy Trust (the "trust") are committed to ensuring that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed by the trust's related schools, business units, subsidiary and central team in accordance with the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

The trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the Local Authority, other schools, educational bodies, children's services, as well as service providers to fulfil its function.

This policy is in place to ensure all staff, trustees and governors are aware of their responsibilities and outlines how the trust complies with the core principles of DPA 2018.

Organisational methods for keeping data secure are imperative and so there are written procedures to support this policy, as outlined on the cover page.

When referring to a location or school, the term business unit or subsidiary can also be assumed.

2 Legal framework

This policy is based on the following legislation:

- Data Protection Act 2018.
- General Data Protection Regulations 2016 (GDPR)
- Protection of Freedoms Act 2012 - when referring to our use of biometric data
- School Standards and Framework Act 1998
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- Code of Practice on Records Management (under Section 46 of the FoIA).
- Environmental Information Regulations 2004.
- Regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

The following guidance is also considered:

- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR), including ICO's code of practice for the use of surveillance cameras and personal information
- DfE (2018) 'Data protection: a toolkit for schools'

3 Roles and Responsibilities

3.1 Data Protection Officer

We are a public body and therefore have a named Data Protection Officer, registered with the ICO.

A DPO can be an existing employee or externally appointed, but must be independent, an expert in data protection, adequately resourced, and report to the highest management level (the board). Where an existing employee is appointed to the role of DPO, their duties must be compatible with the duties of the DPO and not lead to a conflict of interests. To minimise

potential conflicts the trust will appoint an independent DPO where possible. In these circumstances, DPO duties will be delegated to the role of Deputy DPO.

The DPO is appointed in order to

- Advise and monitor the trust's compliance with data protection legislation, including performance of other formal duties as defined by the data protection legislation, DPA (2018).
- Apply knowledge and experience to assist the trust in delivering services.
- Report breaches to the ICO and is the ICO's first point of contact with the trust. Investigate critical major breaches.

Further responsibilities may be delegated to a Deputy DPO, to

- Define and review policy and procedure effectiveness.
- Inform and advise the trust and its employees about their obligations to comply with data protection legislation.
- Monitor the trust's compliance with the legislation and guidance, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.
- Act as the first point for individuals whose data is being processed.

The DPO/Deputy DPO will

- Operate independently and will not be dismissed or penalised for performing their duties.
- Be provided sufficient resources and appropriate access will be provided to the DPO to enable them to meet their UK GDPR obligations.
- Be involved in all data protection matters by staff across the trust and in a timely manner in case of data incidents or potential breaches).

3.2 CEO/Headteacher

The CEO acts as the representative of the data controller on a day-to-day basis, with the Headteachers acting as representatives of their schools and associated business units, ensuring that staff and visitors follow policy and, in the case of breaches, managing communications and any disciplinary proceedings.

3.3 Trust Central Team

The Commercial Director will act as Deputy DPO, driving policy, compliance and training.

The Head of IT will assist in investigation of critical major breaches and subject access requests involving IT.

3.4 School Business Managers

School Business Managers (SBMs) are the primary point of contact regarding data protection for a given school and related business unit. They assist in implementation of policy by ensuring processes are documented and procedures are followed. In some schools this role may be delegated, with approval from the Headteacher. For Business Units this should refer to the Business Unit Lead.

3.5 All Staff (and related parties)

All staff have a responsibility to follow policy. From section 7 onwards, their duties are clearly explained. Most of these duties will also apply to other related parties e.g. volunteers or contractors onsite, if relevant.

4 Data Protection Principles

UK data protection legislation defines principles that all schools, business units and subsidiaries across the trust must comply with. We have a number of data protection-related activity areas (section 8 onwards) and supporting procedures that help us ensure we are compliant with these principles.

4.1 Key Terms

Term	Definition
Relevant data	The scope of data protection relates to the following relevant data • automated personal data • data in manual filing systems, unfiled data (e.g. display items, piles of paper records), where personal data is accessible • chronologically ordered data • pseudonymised data, e.g. key-coded.
Personal data	Any information relating to an identified, or identifiable living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username or IP address It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, facial shape, retina and iris patterns, and hand measurements), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Commercially-sensitive data	Commercial or market sensitive data, including that subject to statutory or regulatory obligations, that may be damaging to GEP Academies, a public body or a commercial partner, if improperly accessed.
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data. This would include all employees of the trust.

Term	Definition
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach or security incident.	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Data Protection Officer (DPO)	Data protection legislation introduces a duty for public authorities to appoint a data protection officer (DPO), who advises and monitor the trust's compliance with data protection legislation.

4.2 Demonstration of Compliance

UK data protection legislation also requires that "the controller shall be responsible for, and able to demonstrate, compliance with" the above principles.

The trust therefore offers new employees initial data protection training and annual data protection top-ups thereafter.

Employees are expected to demonstrate understanding of their obligations regarding this policy by signing a data protection Policy Compliance Declaration.

4.3 Core Principals

The principles say that personal data must be

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure.

a) Processed lawfully, fairly and in a transparent manner

There must be a legal basis by which data is processed (See Appendix 1). Data privacy notices are published to be transparent (see trust website).

The trust will draft consistent privacy notices for schools, covering the following data subjects: Pupils/parents, employees, trustees/governors, volunteers, visitors. Where a school or business unit has additional data subjects that require privacy notices, they are to draft a privacy notice for review by the Commercial Director.

Our privacy notices will be written in clear and plain language and are adapted when addressed to a child; we have a primary school-age privacy notice and a secondary school-age privacy notice.

b) Collected for specified, explicit and legitimate purposes.

It must not be further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research

purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

c) Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.

Further unnecessary data should not be gathered unless required.

d) Accurate and, where necessary, kept up-to-date

Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

e) Kept for no longer than is necessary for the purposes for which it is processed

Personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK data protection legislation, in order to safeguard the rights and freedoms of individuals.

f) Processed in a way that ensures it is appropriately secure.

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.

5 Data Protection Rights

Data protection legislation introduced 6 rights of individuals, as outlined below.

5.1 The right to be informed

Adults and children have the same right to be informed about how the school uses their data.

The privacy notices supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language, which is concise, transparent, easily accessible and free of charge.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, the controller's representative, where applicable, and the DPO.
- The purpose of, and the lawful basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

5.2 The right of access

Individuals, including children, have the right to obtain a copy of their personal data as well as other supplementary information, including confirmation that their data is being processed.

Individuals, including children, have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

Where a SAR has been made for information held about a child, the school will evaluate whether the child is capable of fully understanding their rights. If the school determines the child can understand their rights, it will respond directly to the child.

The school will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning

behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

The school will ensure that information released in response to a SAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data, the school will:

- Omit certain elements from the response if another individual's personal data would be disclosed otherwise.
- Reject requests that cannot be fulfilled without disclosing another individual's personal data, unless that individual consents or it is reasonable to comply without consent.
- Explain to the individual who made the SAR why their request could not be responded to in full.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to – the time limit for responding to the request will be paused until clarification from the individual is received.

5.3 The right to rectification

Individuals, including children, are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

The school will take reasonable steps to ensure that data is accurate or are rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data.

The school will restrict processing of the data in question whilst its accuracy is being verified, where possible.

The school reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

Where no action is being taken in response to a request for rectification, or where the request has been investigated and the data has been found to be accurate, the school will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

5.4 The right to erasure

Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals, including children, have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent where consent was the lawful basis on which the processing of the data relied
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The school will comply with the request for erasure without undue delay and at the latest within one month of receipt of the request.

The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The establishment, exercise or defence of legal claims

The school has the right to refuse a request for erasure for special category data where processing is necessary for:

- Public health purposes in the public interest, e.g. protecting against serious cross-border threats to health.
- Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.

Requests for erasure will be handled free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and them later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

5.5 The right to restrict processing

Individuals, including children, have the right to block or suppress the school's processing of personal data.

In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful, and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where the school is restricting the processing of personal data in response to a request, it will make that data inaccessible to others, where possible, e.g. by temporarily moving the data to another processing system or unpublishing published data from a website.

The school will inform individuals when a restriction on processing has been lifted.

The school reserves the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

5.6 The right to data portability

Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- Where personal data has been provided directly by an individual to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form.

The school will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

The school will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

5.7 The right to object

The school will inform individuals, including children, of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals, including children, have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Processing used for direct marketing purposes
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- The school will respond to objections proportionally, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress.

a) Processing for direct marketing purposes

Where personal data is processed for direct marketing purposes:

- The right to object is absolute and the school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- The school will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.

b) Processing for research purposes

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

c) Objection Procedures

We will record all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings.

We will respond to all objections without undue delay and within one month of receiving the objection; this may be extended by a further two months if the request is complex or repetitive.

Where no action is being taken in response to an objection, we will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

Data Protection Impact Assessments (DPIAs)

6 Education Data Processing

6.1 Safeguarding Information

The school understands that data protection legislation does not prevent or limit the sharing of information for the purposes of keeping children safe.

The school will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible.

Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

The school will aim to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk.

The school will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

6.2 Schoolwork

School work and assessment data is developed both at school and at home by pupils. This work may be held at school or taken home for marking and review by our trust staff, with due care to the security of such data, where personal. Where schoolwork is shared outside of the trust, for example for moderation purposes or best-practice sharing, we will ensure it is de-personalised.

Where schoolwork is not returned to the pupil at the end of the school year, we will archive this based on our data retention procedure. Some work may be considered of important educational or historic value and therefore retained for longer periods.

6.3 Examination data

Examination data is processed in line with instructions from the Joint Council for Qualifications (JCQ).

6.4 Online Services for Children

Where consent is required, parental consent must be obtained for information society services online, at least for all children under 13 (except preventive/counselling services or where a curriculum tool is selected for educational provision).

The ICO advises that if you are relying on consent as your lawful basis for processing personal data, when offering an online service directly to a child, only children aged 13 or over are able provide their own consent. (This is the age proposed in the Data Protection Bill and is subject to Parliamentary approval). For children under this age, you need to get consent from whoever

holds parental responsibility for the child - unless the online service you offer is a preventive or counselling service. To ensure that the child is competent in all cases GEP Academies will rely on parental consent, up to Year 11. We will encourage that this decision is made with the child. In terms of transparency, for all cases of parental consent, we will have a child-friendly privacy notice available. To ensure that all 18-year-olds consent for themselves, from Year 12, students will consent for themselves.

Where we provide online applications as part of its educational provision, we do so under Article 6(1)(e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller as an educational establishment. For the avoidance of doubt, such curriculum tools do not extend to social media sites. With the current advances in technology, educational applications are the chosen way to deliver the curriculum to pupils. Therefore consent (by parent or pupil), is not required.

6.5 CCTV

We use closed-circuit television (CCTV), in most sites across the trust and in various locations around each site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. See Surveillance Procedures.

We understand that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

We notify all pupils, staff and visitors of the purpose for collecting CCTV images via our data privacy notice, as well as school-specific communications.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept as per the Data Retention Procedure guidelines; the school's Data Officer is responsible for keeping the records secure and allowing access, in line with our trust Surveillance Procedures.

6.6 Photography and video footage

As part of our activities, we may take photographs and record images of individuals within our educational sites to assist in the provision of education and safeguarding. Consent is not required for this purpose.

Where we take photos for other purposes, we will always indicate our intentions for taking photographs and will retrieve permission before publishing them.

If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

Precautions are taken when publishing photographs of pupils, in print, video or on the school website, as per school procedures.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the relevant data protection legislation.

6.7 Biometric Data

a) Processing

The following definitions are relevant:

- **Automated biometric recognition system:** A system which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e., electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.
- **Processing biometric data:** Processing biometric data includes obtaining, recording or holding the data or carrying out any operation on the data including disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

We may process biometric data by

- Recording pupils' biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.
- Storing pupils' biometric information on a database.
- Using pupils' biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise pupils.

b) Risk Review

Prior to processing biometric data or implementing a system that involves processing biometric data, a Data Processing Impact Assessment will be carried out. If a high risk is identified that cannot be mitigated, the DPO will consult the ICO before the processing of the biometric data begins. The ICO will provide the school with a written response (within eight weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether the school needs to take further action. In some cases, the ICO may advise the school to not carry out the processing.

Where the school uses pupils' biometric data as part of an automated biometric recognition system (e.g. using pupils' fingerprints to receive school dinners instead of paying with cash), the school will comply with the requirements of the Protection of Freedoms Act 2012.

c) Consent for Pupils

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it. Parent's will be provided with a Parental Notification and Consent Form for the use of Biometric Data.

The name and contact details of the pupil's parents will be taken from the school's admission register. Where the name of only one parent is included on the admissions register, the Headteacher (or delegate), will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent.

The school does not need to notify a particular parent or seek their consent if it is satisfied that:

- The parent cannot be found, e.g. their whereabouts or identity is not known.
- The parent lacks the mental capacity to object or consent.
- The welfare of the pupil requires that a particular parent is not contacted, e.g. where a pupil has been separated from an abusive parent who must not be informed of the pupil's whereabouts.
- It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.
- Parental consent is not required due to age (post-16 students) – see Section 8.1a Post-16 Students.

Where neither parent of a pupil can be notified, consent will be sought from the following individuals or agencies as appropriate:

- If a pupil is being 'looked after' by the Local Authority (LA) or is accommodated or maintained by a voluntary organisation, the LA or voluntary organisation will be notified, and their written consent obtained.
- If the above does not apply, then notification will be sent to all those caring for the pupil and written consent will be obtained from at least one carer before the pupil's biometric data can be processed.

Notification sent to parents and other appropriate individuals, or agencies will include information regarding the following:

- Details about the type of biometric information to be taken
- How the data will be used
- The parent's and the pupil's right to refuse or withdraw their consent

d) Consent for Adults

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

e) Non-participation

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We recognise it is our duty to provide reasonable alternative arrangements for those individuals whose biometric information cannot be processed. We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish or online.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

We will not process the biometric data of an individual in the following circumstances:

- The pupil/adult (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data
- No consent has been received in writing to the processing
- A parent has objected in writing to such processing, even if another parent or the pupil under 18 has given written consent

Parents and pupils, as well as other individuals, can object to participation in our biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

If a pupil objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, we will ensure that the pupil's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the pupil's parent(s).

Pupils will be informed that they can object or refuse to allow their biometric data to be collected and used.

Where staff members or other adults use our biometric system(s), consent will be obtained from them before they use the system.

Staff and other adults can object to taking part in our biometric system(s) and can withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

Alternative arrangements will be provided to any individual that does not consent to take part in the school's biometric system(s). These arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service or result in any additional burden being placed on the individual (and the pupil's parents, where relevant).

If an individual (or a pupil's parent, where relevant) withdraws their consent for their/their child's biometric data to be processed, it will be erased from the system.

6.8 DBS data

All data provided by the Disclosure and Barring Service (DBS) will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated; the results will however be transcribed on our Single Central List.

If DBS data is stored beyond the immediate need, the individual's consent will be recorded alongside.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

7 Information Governance

7.1 Employee and related-party responsibilities

All employees and related parties must consider the following:

- **Compliance:** Comply with the trust Data Protection Policy, by
    - Reading the policy upon appointment or major overhaul
    - Signing to declare agreement to compliance.
- **Training**: Successfully complete relevant training in data protection and key messages annually.

7.2 Line Manager responsibilities

- **Compliance:** All line managers must ensure that employees under their management are complying with trust policies and any agreed exceptions.
    - Managers have a key role in ensuring any policy is being implemented appropriately.
    - Ensure employees have completed relevant formal training (for systems they use, and compulsory e-Learning). Use team meetings to discuss information policy issues. Where there is uncertainty over correct procedure, seek advice for clarification.
    - Any exceptions to Data Protection Policy must be risk assessed and approved

7.3 Trustee responsibilities

- **DPO:** The Board of Trustees must ensure that the role of Data Protection Officer (DPO) is in place.
- **Annual Review:** The Board of Trustees' Audit & Risk Committee must ensure that designated employees and related/ third parties undertake annual reviews of data protection and any associated risks.
    - An annual DPO report will be required.
    - Policy and/or risk reviews should be undertaken annually by the Deputy DPO.

8 Data Processing

We take our duties under the Data Protection law and associated regulations very seriously. Any unauthorised disclosure may result in disciplinary action.

8.1 Employee and related-party responsibilities

All employees and related parties must consider the following:

a) Daily processing activity

- **Emails**: ensure personal information sent or forwarded in emails is only received by the intended recipient.
    - Circular emails to parents or other individuals outside the trust are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
    - Content and attachments are checked for personal information, when sent to people outside of the trust and the data subject themself. School office protocols are in place to clearly identify files containing personal information.
    - Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- **Opinions**: Record opinions or intentions about service users carefully and professionally.
    - A data subject may exercise their rights to ask us to amend or delete their personal data if they feel the validity of comments to be inaccurate.
    - Consider that anything committed to record about an individual may be accessible by that individual in the future (through a Subject Access Request), or challenged over its accuracy
- **Disclosing information publicly or to other adults**: Fully consider Data Protection law before disclosing personal information, when receiving a request from anyone asking to access the personal data of someone other than themselves, or when publishing information, or sharing with third parties.
    - Check the legal basis for disclosing information (See Appendix 1)
    - Consider the extent of information in the public domain.
    - Ensure there is adequate security is in place to protect it.
    - Check that the person receiving the data has been outlined in the trust's privacy notice, as we must be transparent with our data subjects about who we share data with.
- **Post-16 Students**: Ensure information is only disclosed to parents/guardians where consent has been obtained by the student. Ensure the post-16 student's expression of consent (e.g. biometric data processing), is not overridden by prior consent of parents.
    - At age 18, students are legally an adult and therefore any other adult needs their permission to access their personal data. It is therefore the trust policy that all communications regarding personal data of students from Year 12 onwards are directed towards students (not parents), unless explicit consent has been obtained e.g. on Sixth Form application form.
    - Year 12 is set as the threshold for practical reasons, rather than a student's 18th birthday. Schools should be mindful of how to implement this policy where any student is educated in a cohort ahead of their age-related year group.
    - See Appendix 1 for further information on consent.
- **Minimisation**: Process only the minimum amount of personal data necessary to deliver services

- See the data minimisation principle, within section 4.2.

- **Accuracy**: Take reasonable steps to ensure the personal data we hold is accurate, up to date and not misleading.
  - Regular checks should be performed on data held (e.g. through annual pupil/parent, staff, or governor data collection verifications)
  - Data should be checked where contact with an individual is re-established.
- **Data Retention:** Ensure that the personal data they process is reviewed and destroyed when it is no longer necessary. Archive data on an annual basis, according to the Data Retention Procedure.
- **Data protection rights**: Consider a subject's **rights** under Data Protection law when someone contacts them requesting a change to the way their personal data is processed.
- **Access rights:** Ensure that only those with a business need to access personal data are able to do so; never access personal data they have no right to view.
  - Consider technical methods, such as encryption, password protection of systems, restricting access to network folders
  - Consider physical measures, such as locking cabinets, keeping equipment like laptops out of sight, ensuring buildings are physically secure
    - Consider organisational measures, such as
    - Appropriate induction and training
    - Reliability of staff that access personal data, for example, by the use of Disclosure and Barring Service (DBS) checks.
    - Making sure that passwords are kept secure, forced to be changed after an agreed period and are never shared.

b) Advanced processing

- **Privacy Notice:** Ensure that data subjects have access to a complete and current Privacy Notice.
  - The data privacy notice is held on the trust website (See contacts)
  - New pupil admissions, employees and visitors to the trust should be advised of the privacy notice.
  - The data privacy notice should be referenced on key requests for information
  - Pupils should be introduced to the child-friendly data privacy notice by schools
- **Subject Access Requests**: Handle any request from a member of the public or colleagues asking to access their personal data, as a Subject Access Request. See Statutory Request section.
- **Consent:** Where processing cannot rely on any other legal power or condition, consent must be relied upon to process the data. See Appendix 1.
- **Research (Anonymisation):** Follow the relevant procedure, where personal data needs to be anonymised or pseudonymised, for example for research purposes.
  - Follow the guidance in the Data Processing (Minimisation) Procedure.
- **Direct marketing:** Consent must be obtained if personal data is to be used for promoting or marketing goods and services. See section 5.7.

- **CCTV, internet, emails, calls**: Be compliant with the law and the regulator's Code of Practice where the content of telephone calls, emails, internet activity or video images of employees or the public is recorded, monitored or disclosed.
    - The law permits organisations to hold such data in order to measure the quality of services being provided, to record consent etc. In certain circumstances recordings may be accessed e.g. to investigate alleged criminal activity or breaches of trust policy, etc. See the trust's Subject Access Request Procedures.
    - Operation of overt surveillance equipment such as CCTV must always be done in line with relevant codes of practice captured in the Surveillance Management Procedure. Any covert surveillance must be done in line with the provisions in the Investigatory Powers Act (2016). See trust Surveillance Procedure.
- **External Bodies:** Share personal data with external bodies who request it, only if there is a current agreement in place to do so, or it is approved by the Data Protection Officer.
    - The agreement should cover legal grounds for sharing and security measures.
    - Raise a policy exception of no agreement is in place using the service request database (see contacts)
- **Data Privacy Impact Assessment**: Ensure that the risk to privacy rights is formally assessed when introducing any new (or change to an existing) system or process which processes personal data.
    - A data privacy impact assessment should be undertaken, using the trust service request database (See contacts).
- **European Economic Area Hosting/Sharing**: Ensure data will be kept within the European Economic Area.
    - The member states of the EEA share common legislation which provides assurance of equivalent legal safeguards as those under the Data Protection Act.
    - If you are proposing a process or system change which may involve the hosting of personal data in a nation outside the EEA, this must be first approved by raising a Privacy Impact Assessment service request via the trust Service Request Database (See Contacts at the front of this policy)
- **Data matching:** must only use data matching techniques for specific purposes in line with formal codes of practice, informing service users of the details, their legal rights and getting their consent where appropriate.
    - A Data Privacy Impact Assessment should be completed for this activity. (See DPIA Procedures)

8.2 Line Manager responsibilities

- **Training:** Line managers must consider that their reports are trained to an appropriate level, based on their roles and responsibilities, to be able to handle personal data securely.

8.3 Central Team responsibilities

- **ICO Registration:** The Commercial Director will maintain an up-to-date entry in the Public Register of Data Controllers**.**
    - ICO registration to cover all schools, business units and trading names
    - Consider any change to the purposes of processing personal data occurs with SBMs

- **Privacy Notices:** The Commercial Director will maintain data privacy notice for trust-wide activity, as per input provided by schools and business units.
    - Privacy notices for activities undertake, for adult readership
    - Privacy notices adapted for primary / secondary readership.

9 Acceptable Personal Use of Resources and Assets

This section explains what is acceptable use of resources and assets provided by the trust, including IT facilities and covering personal use.

For the avoidance of doubt, where schools or business units within the trust have their own acceptable use procedures or codes of conduct, and there is a conflict, the provisions within this policy will override any local procedure.

9.1 Employee and related party responsibilities

a) Daily processing activities

- **Unattended data:** Must not leave personal or commercially-sensitive information unattended, when printing, photocopying, scanning or faxing. If there is no secure release facility which requires you to be present, you must ensure you wait for the process to complete and remove any originals and copies from the equipment, when sending personal data to a shared or unattended device.

- **Authorised Disclosure:** Must not disclose (in writing, speech or electronically), information held by the trust unless they are authorised to do so, and the recipients are authorised to receive it. If you are not sure if you are authorised to disclose information, speak with your manager in the first instance.

- **Compromised data:** must not do anything that would compromise the security of the information held by us, such as downloading/ spreading any harmful virus/ program or disabling or changing standard security settings.
    - IT controls should prevent your ability to download anything harmful, but if in doubt, contact your manager in the first instance.
- **Personal use:** ensure that personal use of equipment does not reflect adversely on our reputation; not make personal use of the information available to them that is not available to the public, nor let personal use interfere of trust facilities interfere with working time, productivity or how they carry out their duties. Furthermore, the trust's facilities or property may not be used for commercial purposes or for personal financial gain.
    - If you wish to utilise trust data in a personal capacity, you must make a formal request for information to the Headteacher/CEO to do so. In line with the Nolan Principles, this should not provide personal gain.
    - You must only make personal use of our IT facilities outside of time you are recording or is designated as your 'working hours' and with agreement from your manager.
- **Unlawful use:** must not use the trust's facilities or property to undertake any unlawful, libellous, immoral or offensive activities, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to, pornographic, sexual, violent or criminal content and racist, sexist or otherwise discriminatory material.

- **Costs incurred**: use the trust's facilities economically; personal use must not create extra costs for the trust.
    - Check with your manager or where you have any uncertainty over what is appropriate.

b) General code of conduct

- **Personal browsing in company time**: ensure not leaving personal-use websites open during working time, even if they are minimised on the screen and they are not actively viewing/ using them.

- **Unacceptable browsing**: ensure no use of browsers or access/ attempt to access sites that are knowingly unacceptable, whilst on premises of the trust or with trust equipment on/ off-site, even if this is in their own time.

- **Email spam**: must not send or forward chain, joke or spam emails with Trust email accounts. These should be deleted if received.

- **Unauthorised devices**: must not connect any equipment that has not been approved by IT to a network within the trust.

- **Role abuse**: ensure no use of access rights or identity as an employee/ representative of the trust to mislead another person, for personal gain or in any other way which is inconsistent with their role.

9.2 School Business Manager / Business Unit lead responsibilities

- **Equipment Register**: Ensure there is a process to sign out, with the appropriate authority, any trust equipment being taken off-site and return the equipment when requested, no longer required or when employment/tenure ends, whichever is first.
    - Use of trust equipment off-site should be approved by a line manager, IT Team and/or School Business Manager.
    - A register of assets on loan should be maintained at each location.

10 Data Handling Security

Responsibilities for managing IT equipment, removable storage devices and papers, in the office, in transit and at home or other work locations.

10.1 Employee and related-party responsibilities

All employees and related parties must

a) Daily processing activity - onsite

- **Portable storage devices:** ensure that memory sticks are only used to hold personal information if they are password-protected, fully encrypted and carefully looked after. It is preferable not to use such mobile storage devices at all.

- **Confidential conversations:** make sure that conversations discussing sensitive data are only audible by an **appropriate audience**.
    - We have a duty even within our premises to make sure that personal data is only made available to those with the business need to access it. This applies verbally as well as in recorded form.
    - Most employees who handle personal/commercially-sensitive data will have been located with those of similar roles or be in self-contained spaces. However, there is always the possibility of unauthorised persons being in the vicinity when you may need to discuss personal/commercially-sensitive data with colleagues near you or over the phone, or display on a screen.
    - You must make sure as the person who is custodian of the information that it is appropriate to discuss or display the information in the circumstances. You must make sure that if you are overhearing or otherwise being exposed to data to which you should not have access, you alert the information custodian to the fact that they are not managing the information appropriately.
- **Unauthorised access:** Employees and related parties must not allow unauthorised people to be able to access confidential records or view information on their IT equipment display.
    - Unauthorised people may be able to see personal/commercially-sensitive data information on your screen or access this information if accessing the building (e.g. parents, lettings, service contractors).
    - Keep confidential paper records in a locked filing cabinet, drawer or safe, with restricted access. Do not leave confidential paper records unattended or in clear view anywhere with general access.
    - Ensure that no-one in your vicinity can see and read the screen of your device. This applies to working in public places (such as cafes with Wi-Fi), in partner organisations' offices, and even when hot-desking within our premises when viewing personal/commercially-sensitive data unless you are certain that others around you are allowed to see similar data.
- **Others using your device**: Ensure no one is allowed access to their trust IT equipment through their IT account.
    - All activity on your IT account is assumed to be yours. Logs of activity are maintained. You are accountable for any wrongdoing through your account.
    - Lock your screen at all times if you leave your laptop/ desktop or phone unattended to avoid someone accessing your account without your knowledge.
    - Always supervise and monitor anyone using your device in the strictly limited circumstances where allowing someone access is acceptable (for example a Network IT Technician may need to review your account).

- **Unapproved equipment:** ensure you do not use any equipment to store the trust's personal or commercially-sensitive data that has not been approved. Remove data once finished working with trust data on approved unmanaged equipment.
    - Equipment purchased through us will have appropriate technical security installed, or will have best practice guidance on how to use the equipment securely.
    - This is including but not limited to computers, printers, phones, tablets and cameras. Order equipment through us and follow any conditions of use associated with an "exception to policy" and follow any standard instructions that are supplied with the device. Where technically feasible, encryption will be applied to secure the contents of storage devices, thus enabling them to be locally approved.
    - Data in the browser cache or temporary file storage may be useable by other subsequent users of the same device.
    - On most systems this can be done by selecting 'public network' when setting up the access. Otherwise, it will need to be done manually in the web browser options. When deleting data on a device, care should be taken to permanently delete, to ensure it is also removed from the trash bin.
- **Web Password: Employees and related parties** must not save their password in the browser, when using their school/trust email account or any work-related application, when using **Web Access** from an unmanaged device, or when using a generic/ guest login.
    - This introduces the risk of someone who can gain access to your device also getting easy access to the data on your work emails.
    - Do not approve any offer from your device's browser to save your password when logging in.
- **Equipment care**: take responsibility for the security of the equipment allocated to them and that is in their custody and keep their portable equipment clean and serviceable, including keeping it charged.
- **Lost equipment:** report as quickly as possible if their equipment is lost or stolen and assist with any investigation.
    - This enables us to promptly remove data from devices remotely, therefore reducing the risk. Such investigations may lead to disciplinary action, and in extreme circumstances could lead to the service area seeking financial remuneration. Having all the information about a security incident helps us to resolve it quickly and take the appropriate action to manage any risks of information being lost.
    - Raise a security incident via the trust Service Request database and inform your manager. Provide any information requested of you by an investigating officer.

b) Daily processing activity - offsite

- **Transportation:** take steps to keep data secure when physically transporting Trust data outside of the trust premises, on any medium. Mobile devices holding personal or commercially sensitive data must be encrypted.
    - Prevent any accidental loss (for example papers or removable media accidentally falling out of bags), or theft (by exposing papers or equipment by not securing them properly).
    - This relates to paper files, phones, laptops and other removable media such as USB memory sticks, discs and external hard drives. Use equipment which

reduces physical effort in order to appropriately manage the risk of overloading or forcing a tenuous hold over physical documents which can result in accidental loss of control over the information (for example: use folders for loose papers; use bags, (wheeled) briefcases for multiple folders).
    - Items should not be visible to others; even partially. This means they should be secured within an appropriate bag or other robust container. Laptop bags are suitable, ensuring that zip compartments are closed concealing the contents.
    - Employees frequently needing to transport quantities of information that are too bulky to carry under full control and/or transporting personal/commercially-sensitive data must review with their manager the need for being supplied with wheeled suitcase-style equipment with code locks to further secure the information.

- **Home security: All employees and related parties** must take appropriate steps to secure Trust data at **home** and at other organisations' **premises.**
    - Only authorised users (this means people with IT accounts provided by us) can use your IT equipment and only through using their own accounts. It is not acceptable to allow family members or friends to use IT facilities or have access to our information even if you are present.
    - You must also make sure that when IT equipment and hard-copy information is not in use, that it is stored securely out of sight. If you are located temporarily in the premises of another organisation or your work requires site visits or entering homes of service users, you must secure IT equipment and hard-copy information.
    - Your role may require you to allow someone to have access to your IT device, for example a service user in their home may need to read content on your screen and select options from menus. You must understand the limits of their access requirements and manage this access.
    - If you are located in the premises of another organisation as a semi-permanent base, it is reasonable to leave our data in your allocated office or team area provided that you have the same level of secure storage for equipment and hard-copy as you would in our buildings. You must get approval for storing our data in premises not managed by us from your manager if the location is anything other than your permanent office base.

- **Vehicles**: ensure personal data or commercially-sensitive data is not left unattended in a vehicle for longer than 10 minutes; always keep it out of sight.
    - Experience in investigation of thefts at employee homes has shown that if equipment is left in plain view, it will be taken, whereas storing away out of sight when not in use results in fewer cases of theft. In the first 10 minutes a car left unattended is far less likely to get broken into than a car left unattended for over this duration. This threshold is set for the circumstances where taking all personal/commercially-sensitive data items is impractical, to strike a balance between inconvenience and risk.
    - Locked in a boot is considered secure for a limited time if it cannot be taken with you when leaving a car.

- **Abroad:** must not take any of the Trust's equipment abroad unless they are travelling in a business capacity with approval.
    - We need to be aware of any risk of using our equipment abroad, especially in countries who do not share common legislation to safeguard personal data, and where internet services may expose our devices and therefore our network to malicious threats. There may also be costs involved in replacing equipment which is subject to precautionary measures on your return. The costs of reviewing requests and replacing equipment are not appropriate for instances

of employees wanting to use equipment whilst on holiday. Business continuity cover arrangements and delegation should be able to manage instances of leave.
    - Request an exception to policy via the trust Service Request database to have your case considered.

- **Sharing devices:** must not give their assigned portable equipment to another person if they are not using it.
    - Portable equipment is asset managed across our estate and assigned to an individual. Being able to accurately evidence who holds what equipment is an important assurance we give to the Information Commissioners Office over our ability to manage our assets and the information available on them.
    - Ensure that any equipment given or received by you is through our processes of managing assets, as defined by your School Business Manager.

10.2 **School Business Manager responsibilities**

- **Business Continuity**. Develop business continuity and recovery measures, including those relating to protecting data; invoke these measures when a security incident arises. See Risk Management Policy.

- **Offsite data system:** Provide a system for recording personal information being taken off-site. This could be managed through recording of processing activities.
    - It is important to make sure that others know who has custody of important information at all times.
    - You should have access to systems or a log which allow you to 'sign-out' or record what information you are taking custody of, when taken, when returned and (if appropriate) why and under whose authority. Where such facilities are available, they must be used. Where this is conducted on a regular basis, this should be recorded in your Record of Processing Activity. Otherwise, one school-based asset log should be maintained in accordance with guidelines set by your School Business Manager.
- **Secure disposal:** All employees and related parties must always use an approved secure method of disposing of physical documents and data storage devices.
    - Secure destruction processes safeguard the information stored on IT devices and physical documents and prevent data being accessed by unauthorised persons.
    - Make use of the facilities for secure disposal of paper documents and IT storage devices. All sites are to provide facilities for the secure disposal of paper documents and IT storage devices by contractors with appropriate data sharing agreements in place.
- **Equipment return:** ensure there is a clear process for the return all equipment which has been issued to individuals by the trust, prior to leaving their employment, term of office or contractual arrangement.
    - Providing such items is costly and represents a data security risk. We reserve the right to treat instances of refusing to return such items as theft.
    - As part of your own leaver's checklist process, ensure you review equipment with your manager.
- **Monitoring of data security:** test, assess and evaluate the effectiveness of any and all measures in place for data security on a regular basis, in conjunction with the premises and IT leads onsite.

10.3 IT Team responsibilities

- **Network security**: ensure networks are designed with necessary security measures in mind, regularly tested for cycler attacks; backed-up on a regular basis with retrieval mechanisms tested.
    - Consult the trust Head of IT for all security, encryption and password protection protocols
- **Device security**: issue devices with appropriate security measures in place to protect data.
    - All electronic devices are password-protected to protect the information on the device in case of theft.
    - Where possible, enable electronic devices to allow the remote blocking or deletion of data in case of theft.
    - Provide all necessary members of staff with their own secure login and password; ensure every computer regularly prompts users to change their password.
- **Ensure employees are trained on** all enabling security functions on their portable equipment, such as pin codes and password access.

11 Records Management (Retention)

Responsibilities for management of information to support secure access and effective retention, destruction and preservation processes.

- Data will not be kept for longer than is necessary.
- Unrequired data will be deleted as soon as practicable.

11.1 Employee and related party responsibilities

a) Daily activity

- **Appropriate audience:** ensure that the information they manage is only known to an appropriate audience.
    - You must ensure that paper files are accessible to authorised colleagues in your absence, by ensuring others know where to find keys to lockable storage areas.
    - You must be aware of who information should be shared with, and ensure it is only shared with that audience.
    - You must ensure that you save electronic information in a shared environment, but with appropriate access controls if the information has a restricted audience.
- **Encrypted Devices:** Ensure personal or commercially-sensitive information is stored on an encrypted device if mobile.
    - By only storing all business information on the relevant systems designated by the trust and by using only equipment approved by the trust.
    - By only storing personal/commercially-sensitive data on mobile devices which have been encrypted according to trust guidelines (or on devices which are permanently based at the trust, with appropriate security measures in place).
- **Email storage:** Follow good practice for managing email when storing emails as records, being aware that such emails could be subject to a Subject Access Request.
    - Follow the best practice guidance and any superseding amendments made by the Trust.
- **Data Retention**: ensure that all information in any format which they hold as a record of the trust's activity must be retained in line with trust Data Retention Guidelines and best practice. This will also assist with making best use of the available storage space.
    - Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained

b) Advanced processing

- **Pupil records**: manage pupil records in line with best practice and specific system guidance.
    - Follow the best practice guidance and any superseding amendments made by the trust: Data Retention Guidelines
- **Records of Processing Activity:** document their work activities in line with procedures, including retention periods (See Record of Processing Activity Procedure).
    - In order to comply with the Section 46 Code of Practice, we must ensure that we are destroying all related information across all formats. For example, destroying a paper file on a project but keeping all the electronic documents

about the project in a shared network folder can cause problems if a Freedom of Information request is received. The request co-ordinator assumes that as the paper file is destroyed then we do not hold any information and responds accordingly. We would then be in breach of the act.

- Employees are aware of best practice requirements and any guidance on use of specific systems through training and communications. A Record of Processing Activity should be maintained to document work activities for this purpose.

11.2 **School Business Manager responsibilities**

- **Historical value**: consider a selection procedure for identifying, reviewing and managing records with historical value, as appropriate.
    - When information is due to be destroyed, there should be a final review to select records for transfer to the Trust's central archiving facility.
- **Supplier selection:** Ensure use of a commercial storage provider or shredding company is assessed, to ensure the right security provisions are place and good value for money. An appropriate agreement must be in place, covering data protection responsibilities.

11.3 **IT Network Team responsibilities**

- **Electronic storage:** ensure that the facilities available for storing and managing information meet legal requirements and best practice, with IT network staff focusing on electronic storage.
    - Approve and regularly review facilities such as systems and physical storage as appropriate against security requirements in Data Protection Law, and all employees must help maintain security standards by following procedure.
- **Equipment data cleaning**: when IT equipment is de-commissioned for use in schools the IT Network team will ensure it is cleansed of personal data before being donated elsewhere, or securely destroyed with an approved provider.

12 Statutory Requests for Information

The trust publishes a publication scheme on its website outlining classes of information that will be made routinely available, however there may be occasion where requests are made for personal data under a Subject Access Request, environmental data, or public data under a Freedom of Information Request. These will be recorded in trust systems, coordinated by a request co-ordinator and performance against deadlines reported to the board

This section details requirements for managing requests for information to comply with the Freedom of Information Act 2000 (FOI), the Environmental Information Regulations (EIR), the Data Protection Act 2018 (DPA) and General Data Protection Regulations 2016. See separate Freedom of Information Policy.

12.1 Employee and related party responsibilities

- **Recording SAR/FOI/EIR requests:** Raise requests via the trust Service Request database immediately upon receipt, so that request co-ordinators can correctly identify the law which applies to the information being requested and manage the request in compliance with that law (which is annually reported to the Audit & Risk Committee). Further resource can also be assigned to assist at this stage.
    - The requestor does not have to specify under what legislation they are making a request. It is our responsibility to correctly identify which legislation applies.
    - Follow procedures to identify request type (FOI, EIR or DPA/GDPR) and log via trust Service Request Database.
    - We must record performance against the statutory deadlines to ensure we are aware of how well we are complying with the law and to help make changes to processes if necessary.
- **Co-operation**: promptly provide all relevant information to a request co-ordinator if asked for it, so that a response can be drafted within the required timescale.

12.2 SBMs or delegated request coordinator responsibilities

- Request co-ordinators should release information unless there is a legal justification for withholding it.
    - We serve the public. We should not hide information from them. The Acts are intended to make us more accountable to the public, to make our processes more transparent, and to encourage the public to trust us. Information should be released unless we can justify withholding it (embarrassment is not a sufficient reason to withhold information). In some cases, we may have to release non-personal information because it is in the public interest although it might otherwise have been considered exempt. Also, it is a legal offence to deliberately withhold or destroy requested information where there is no legal reason to do so.
- Request co-ordinators must clearly and fully explain the reasons why they ever refuse to provide information.
    - We will not be obliged to provide all, or part of the information requested if a legal justification applies. If we believe a reason does apply, then we must help the public to challenge our decisions effectively by giving our reasons and doing so clearly and fully in line with the requirements of the Acts. This is a legal requirement.

    - Ensure the employee making decisions about what can be released and drafting the response has access to legal guidance in order to make the response full and compliant with the law; follow trust templates.

- **Requestor Assistance:** provide advice and assistance to people making a request.
    - Why: The Acts require us to assist requestors, especially where we may be considering refusing a request, in guiding the requestor on how to clarify or re-scope their request to achieve the best outcome. This is a legal requirement.
    - How: Discuss the likely response with the requestor if their request is likely to be refused and explain options that would help them receive as useful a response as possible within the limits of the law. Although we should not ask requestors what they intend to do with the information they have requested, we can explain what we do hold and what is likely to be disclosable to them.

- **Prompt replies:** always try to reply as quickly as possible, but always within the legal deadline.
    - Subject Access Requests (DPA 2018): one calendar month, starting from the day they receive the request. If the organisation needs something from you to be able to deal with your request (e.g. ID documents), the time limit will begin once they have received this.
    - The laws provide statutory deadlines for responding to a request
    - Freedom of Information (FOI) & Environmental Information Regulations (EIR): 20 working days
    - The laws expect information to be well managed and accessible, therefore there is an assumption that requests should be routinely responded to well in advance of the deadline.

- **Response format**: provide the information in the format requested by the applicant, where reasonable and practical.
    - The acts duty on us to provide information in a format that the requester would find most convenient to their needs. We may refuse unreasonable demands and charge in certain cases, but in principle the requestor should be able to receive the information in the way they specify.
    - There must be strong prohibitive reasons not to provide information in a format that is within our ability to provide. Conversion to a new format is however different to having to significantly edit and rearrange information to make it legible in the format requested. Under the latter circumstances, a refusal may be valid, but advice should be sought if unsure.

- **Charges:** must ensure any charges made, are done so in accordance with a published charging policy.
    - The laws require us to make clear the basis for charging to ensure that charges are fair and un-obstructive. We must tell requestors whether a charge applies before we provide the information and we should tell them what that charge will be. Whilst subject access requests can usually be provided free of charge, GEP Academies finds the threshold of 4 hours to be manifestly profound, and therefore an hourly rate is charged beyond this threshold.
    - It is not lawful to charge for information without a published policy explaining the basis for arriving at a fee. In the absence of a published policy, charges are not made.

- **Internal review process:** tell the requestor about our internal review process, when responding to a request.
    - It is a requirement of the act to have an internal review process. Where a requestor expresses dissatisfaction with a response, this must be treated as a

complaint. The act states that expressing dissatisfaction is enough to require us to treat it as such. The ICO requires us to complete the internal review process before it will accept an escalation of a complaint to their office.
    - We choose to manage complaints (known as Internal Reviews) within 20 term-time days. Where a simple error has been made in the response it may be that the issue can be resolved informally. If not, then a full review of how the request was handled is required. This must be undertaken by an employee who was not involved in drafting or approving the original request, although the employee drafting the response may discuss how the original request was handled with those involved.

- **ICO Complaint**: Advise the requestor, when responding to a complaint, that they may complain to the ICO if they remain unhappy with the outcome.
    - This is a statutory requirement.
    - Ensure that the contact details for the ICO are provided to the requestor on any response documentation and explain when it is appropriate to escalate a complaint to the ICO in order to make requestors aware of their rights.

12.3 Central Team

- **DP Support**: The Commercial Director will provide data protection advice and support to request co-ordinators as required e.g. on SARs and including the gathering of trust-wide responses for FOI.

- **IT Support**: The Head of IT will provide IT support to SAR request co-ordinators as required.
    - Retrieving data from all information systems across the trust – for example software systems, all network drives and all employee email accounts.
    - Providing an electronic account for the applicant to view this data for a time-limited period

- **Compliance Monitoring**: The Commercial Director will monitor and report to the Audit & Risk Committee on compliance to meeting statutory deadlines for statutory information requests.

13 Security Incidents

A security incident is a confirmed breach, potential breach or 'near-miss' breach of one of GEP Academies Data Protection & Information policies.

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

The trust does not seek to implement a 'blame culture' and encourages the reporting of all health and safety incidents and concerns without fear of consequences. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself. This could impact both the trust/school and the individuals concerned.

We will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by mandating data protection refresher training where the breach was a result of human error.

13.1 Employee and related party responsibilities

- **72-hour timescale**: Immediately report the discovery of a security incident (refer to the Security Incident Procedures).
    - Capturing security incidents allows us to respond effectively when something has gone wrong. Capturing all types of security incidents allows us to understand where our weaknesses are, how well our policies are working and what we should change about our policies to make them more effective The General Data Protection Regulation sets out strict timescales for reporting to the ICO – within 72 hours of discovery. Where data subjects are at risk, timely action is necessary.
    - Raise a Security Incident service request through the trust Service Request database. No action will be taken against any member of staff who reports a security incident about another member of staff in good faith.
- All employees and related parties must provide as much information as possible when reporting the incident, by completing the online incident report.
    - Why: To help us quickly assess the severity of the incident and to speed up the investigation.
    - How: Include full details of the incident such as dates, names and any remedial action that has been taken.
- All employees and related parties must co-operate with investigations, comply with the timescales and escalation process outlined in our trust Security Incident Procedures.
    - Why: Ensure that all incidents are handled in a timely manner.
    - How: Follow the process outlined in the GEP Security Incident Procedures.

13.2 School Business Manager responsibilities

- **Investigation Oversight:** Oversee and support each investigation for their site and ensure a full record is maintained from initial reporting to closure, including the investigation outcome report**.**
    - Carry out an effective process appropriate to the severity of the incident
    - Follow the process outlined in the Security Incident Procedures. The SBM will decide whether to investigate personally, or to allocate to the line manager/

investigating officer. The SBM will work with the DPO, Commercial Director and GEP IT Manager to investigate major security incidents. For all investigations they will review the outcome report and ensure they are satisfied that the appropriate action has been taken.

- **Investigation Officer:** Assign and Investigating Officer/ Line Manager to complete investigations as directed and complete an outcome report (see Security Incident Procedures).
    - Carry out an effective process appropriate to the severity of the incident.
    - Follow the process outlined in the Security Incident Procedures. This will involve: identifying expected outcomes, stakeholders and any policies breached; speaking to staff and recording evidence; managing risks and putting in new controls to prevent reoccurrence; completing an Incident Outcome Report, held on the trust Service Request Database

13.3 Headteacher/CEO responsibilities

- **Communications and disciplinary action**: support by handling communications and disciplinary actions, as necessary, for their site.
    - As per the process outlined in the Security Incident Procedures, where appropriate for their school the Headteacher (or CEO for multiple schools/central breach), will (1) Develop and implement a communications plan and inform data subjects (service users, staff) (2) Manage disciplinary action.
    - In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, we will notify those concerned directly. In the event that a breach is sufficiently serious, the public will be notified without undue delay. Please see advice of (Deputy) DPO for risk categorisation.
    - Where notifying an individual about a breach to their personal data, we will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.

13.4 Central Team

- **Detection:** The Deputy DPO will design effective and robust breach detection, investigation and internal reporting procedures, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

- **Support**: The Deputy DPO will triage all incidents and support investigations, with advice including remedial actions relating to the incident.
    - Ensure that there is appropriate resource, expertise and independent scrutiny of processes for higher impact incidents, including involvement of Network IT support, as appropriate.
    - Follow the process outlined in the Security Incident Procedures.
    - Assess on a case-by-case basis the risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis, in consultation with the DPO.
    - Ensure all incidents are reported to the DPO for ICO reporting clearance, within the 72-hour timeframe and to the CEO regularly

- **Reporting**: The Commercial Director will undertake ongoing reporting and trust-wide preventative actions.
    - Prepare communications for the ICO. Within a breach notification to the supervisory authority, the following information will be outlined:

        - The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
        - The name and contact details of the DPO
        - An explanation of the likely consequences of the personal data breach
        - A description of the proposed measures to be taken to deal with the personal data breach
        - Where appropriate, a description of the measures taken to mitigate any possible adverse effects
    - Assess risks for trust-wide policy/procedural changes and training needs
    - Report incidents on an annual basis to the DPO and Audit & Risk Committee

13.5 DPO responsibilities

- **Support** the investigation of major and critical incidents; review all other incidents
    - The DPO to undertake the investigation (critical only); DPO to work with Commercial Director / Head of IT and Local SBM's as appropriate (major only).
    - The DPO will assess the necessity to report to the ICO, review the outcome report and recommend any further remedial actions.

14 Appendix 1: Lawful Processing

The legal basis for processing data will be identified and documented prior to data being processed.

14.1 Generic Conditions

Under the relevant data protection legislation, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained
- Processing is necessary for a contract held with the individual, or because they have asked the school to take specific steps before entering into a contract
- Processing is necessary for compliance with a legal obligation (not including contractual obligations)
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for protecting vital interests of a data subject or another person, i.e., to protect someone's life
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

We will only process personal data without consent where any of the above purposes cannot reasonably be achieved by other, less intrusive means or by processing less data.

14.2 Sensitive Data Processing

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
    - Reasons of substantial public interest with a basis in law which is proportionate to the aim pursued and which contains appropriate safeguards.
    - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services with a basis in law.
    - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.

- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law.

Where the trust relies on:

- 'Performance of contract' to process a pupil's data, the school considers the pupil's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a pupil's data, the school takes responsibility for identifying the risks and consequences of the processing and puts age-appropriate safeguards in place.
- Consent to process a pupil's data, the trust ensures that the requirements outlined in section below are met, and the school does not exploit any imbalance of power in the relationship between the school and the child.

14.3 Consent

Consent must be a positive indication expressly confirmed **in words**. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. These are known as consent requirements.

Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told.

We ensure that consent mechanisms meet the standards of the relevant data protection legislation. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent can be withdrawn by the individual at any time.

Where we opt to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined above, the school obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children. See section 6.4.

In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, taking into account the requirements outlined above.

14.4 Automated decision making and profiling

We will only ever conduct solely automated decision making with legal or similarly significant effects is the decision is:

- Necessary for entering into or performance of a contract.
- Authorised by law.
- Based on the individual's explicit consent.

Automated decisions will not concern a child nor use special category personal data, unless:

- We have the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest.

We will conduct a DPIA for automated decision making to mitigate risk of errors, bias and discrimination.

We will ensure that individuals concerned are given specific information about the processing and an opportunity to challenge or request a review of the decision.

Individuals have the right not to be subject to a decision when both of the following conditions are met:

- It is based on automated processing, e.g. profiling
- It produces a legal effect or a similarly significant effect on the individual

We will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, the school will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.