Brighter Futures Academy Trust

Data Protection Policy

(incorporating an elementary guide to GDPR)

Version	**12/20**
Name of Policy Writer	**EducateHR Ltd**
Last Updated	**December 2020**
Next Review Due	**December 2021**

Contents **Page**

1. Introduction

1.1 It is necessary for the academy to collect certain information, or data, relating to those persons with whom it engages, to enable it to function in an effective manner. Such data will necessarily include **personal data** and, in certain circumstances, **sensitive (or special category) data** (these concepts being defined later in this policy).

1.2 In addition to its own immediate requirements the academy may be obliged by law to collect certain specified information to comply with the requirements of relevant central government departments.

1.3 The academy is registered as a **data processor** (again further defined later in the policy) meaning that it is legally responsible for handling (defined as both storing and processing) such information in accordance with legislation.

1.4 Those individuals whose personal data is likely to be processed by the academy will for the most part fall within one of two principal categories, namely **workforce** (this term may, for these purposes, include governors and trainees etc as well as paid employees) and **pupils/students**. The data held for these two categories of individuals will necessarily be of a different nature.

1.5 Additional categories of persons for whom such data may possibly also be held are likely to include individuals such as parents/carers, volunteers and, in certain circumstances, external contractors and/or consultants plus any other persons either providing services to, or receiving services from, the academy.

1.6 All personal information held by the academy will be stored and handled in accordance with relevant legislation including (but not limited to) the following:

- The General Data Protection Regulation (GDPR)
- The Data Protection Act 2018 (DPA)
- The Freedom of Information Act 2000 (FOI).

1.7 In the event of the academy contracting with third parties (such as payroll providers, external HR resource providers and recruitment agencies etc) who are required to process personal data appropriate measures will be taken to ensure that the third party is compliant with relevant aspects of GDPR.

1.8 Observance of the preceding clause will involve additional responsibilities if any data is held in, or transferred to, any country which is not within the European Economic Area (EEA) and this could potentially include the use of cloud-based service providers or web hosting services registered outside the EEA, or even, at least in theory, emailing parents (or third parties) similarly located.

1.9 The academy will also have regard for guidance issued by The Information Commissioner's Office (ICO) (whose contribution to this policy is acknowledged) including 'Overview of the General Data Protection Regulation (GDPR)' and 'Preparing for the General Data Protection Regulation (both issued in 2017). Contact details for the ICO are provided in section 16 of this policy.

2. Purpose and scope

2.1 In the course of their work many academy employees will be required to take part in the acquisition, recording, handling, storage, and processing of personal data and this must always be in accordance with relevant legislation as outlined above.

2.2 This policy will help those employees to understand the meaning and significance of such legislation in relation to assisting the performance of the practical duties of their employment.

2.3 This policy will also clarify individual employee responsibilities as a means of ensuring that the academy (as the data processor) always remains compliant with the law.

2.4 Similarly, the academy will ensure that (in addition to those employees directly involved in the handling (etc) of data) all members of staff, governors, volunteers, trainees, external contractors and/or consultants and any partners of the academy who may have access to any personal data will receive appropriate information and/or training to make them fully aware of their individual and corporate responsibilities in this regard.

2.5 Such training will include making all employees (and others listed in the preceding clause) aware that breaches of data protection legislation have the potential to expose both the individual and the responsible organisation to possible legal action (both criminal and civil).

3. GDPR background

3.1 The General Data Protection Regulation (GDPR) is a regulation in European Union (EU) law which represents a new framework for data protection and privacy legislation throughout the EU. It replaced the previous (1995) data protection directive, upon which current UK law is based.

3.2 The primary aim of GDPR was to give control over personal data back to individual citizens and residents of the EU by conferring certain protections on all (in the form of a new set of 'digital rights') whilst additionally addressing the issue of export of personal data outwith the EU.

3.3 GDPR extended the scope of EU data protection law to all foreign companies processing data of EU residents and thus provided for harmonisation of data protection regulations throughout the EU.

3.4 GDPR was adopted by the EU on 27 April 2016 and became enforceable by the Information Commissioner's Office (ICO) from 25 May 2018 in the UK, on completion of a transition period lasting two years which was agreed by the constituent countries of the EU.

3.5 GDPR has therefore been directly applicable from the above date, upon which it replaced pre-existing UK legislation, principally the Data Protection Act 1998 (although a parallel Data Protection Act 2018 subsequently enshrined this legislation in UK law to ensure its continuing relevance following Brexit).

3.6 The inception of GDPR represented a significantly stricter data protection regime with severe penalties for non-compliance potentially reaching to 4% of worldwide turnover or €20 million, whichever is higher.

4. GDPR rights

4.1 GDPR confers certain rights on an individual. These rights (which, in comparison with the pre-existing DPA, are either new or enhanced) are itemised in further detail in Appendix 1 and include the following:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object.

5. GDPR principles

5.1 Under GDPR, the data protection principles set out the main responsibilities for organisations. These six guiding principles (outlined below) are not dissimilar to those contained within the pre-existing version of the DPA, although with some added detail.

5.2 In relation to personal data, these principles are that this must be:

i. processed lawfully, fairly and in a transparent manner

ii. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (although further processing for: archiving purposes in the public interest; scientific or historical research purposes; or statistical purposes; is not considered to be incompatible with the initial purposes)

iii. adequate, relevant and limited to what is necessary (in other words proportionate) in relation to the purposes for which it is processed

iv. accurate and, where necessary, kept up to date: every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is rectified (or, if more appropriate, erased) without delay

v. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which their data is processed, although once again personal data may be stored for longer periods (subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals) insofar as it may be processed solely for: archiving purposes in the public interest; scientific or historical research purposes; or statistical purposes.

vi. 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.

5.3 One significant addition to historic DPA principles is imposed by GDPR, and this is the issue of accountability. This links to the allied concepts of ‘privacy by design’ and ‘privacy by default’, which should represent axiomatic considerations in all aspects of data protection.

5.4 The principles of privacy by design, and privacy by default, should be observed throughout, and this implies building such considerations into data processing operations and systems from the outset, rather than taking account of data protection as an afterthought.

5.5 In relation to transparency, GDPR specifies that the organisation which processes (which includes merely holding) personal data will 'be responsible for, and be able to demonstrate, compliance with the principles', therefore the academy (the data controller, as defined below) is required to document and evidence compliance, and this represents a significant difference from DPA 1998.

5.6 The academy will uphold the principles of accountability and transparency by documenting decisions taken in relation to a processing activity to satisfy the above requirement, which will be addressed by the academy undertaking to put in place and maintain:

- appropriate technical and organisational measures to ensure that data is processed in line with the principles set out in GDPR, and that such adherence is clearly evidenced
- comprehensive and transparent privacy policies and notices (the availability of which will be freely advertised)
- internal records of processing activities which will include details of the following:
    i. the justification under which any personal data is held and the purpose of data processing relative to each respective justification
    ii. the various categories of personal data held
    iii. retention schedules for these various categories of data
    iv. details of any (third party) recipients of personal data
    v. itemisation of technical and organisational security measures in place
    vi. details (where applicable) of transfers to non-EEA (European Economic Area) countries, including documentation of appropriate transfer mechanism safeguards in place.

5.7 In relation to the processing of personal data it is anticipated that in relation to data obtained and held for pupils/students (and their parents/carers) the justification for such processing will almost invariably be a requirement to carry out obligations under the academy's duty to provide educational provision, whereas in relation to data obtained and held for the academy's workforce the justification for such processing will almost invariably be a requirement to carry out obligations under employment law (applicable to staff members holding a contract of employment) and/or other legal obligation (applicable to governors etc).

5.8 These justifications (the basis on which the data is legitimately processed) will be documented in the academy's privacy notice (which will appear on the academy's website, by which means it will be freely available to interested parties) and the academy's information asset register will also be annotated to reflect this understanding.

5.9 Certain information which schools may previously have habitually gathered (either with or without valid consent) may be peripheral to business needs and in the event that such data is held the academy will therefore require either to obtain suitably informed consent (if a sound case can be made for the material currently held to be retained) or to delete such material from the information asset register. Examples of such information might include data obtained from parents in relation to checking eligibility for free school meals etc, although it should be noted that any financial records linked to pupils or parents may require to be retained for seven years in accordance with legal regulations.

5.10 If the academy is unclear about the range and extent of personal data held it may be appropriate to undertake an audit of relevant information to clarify both the extent and type

of data on record, and to assess whether all such data is up to date (and/or obtained by legitimate means), before coming to a decision as to which categories of data can be lawfully processed, cleaned up or deleted in accordance with GDPR legislation.

5.11 Where deletion of superfluous data requires to be undertaken, care must be taken as this can prove problematic in certain IT systems, and staff carrying out this task must always be alert to such issues. Similarly, when uploading information to the school website staff must always be considerate of any metadata or deletions which could be accessed in documents and images on the site.

5.12 Anonymisation of records (such as assessment records of pupils) may be desired, as a means of preserving the facility to compare performance over several years, but once again this can cause similar technical difficulties.

5.13 Irrespective of the above caveats, the academy recognises its responsibilities under GDPR to observe the principles of data protection by limiting the volume of personal data held to the justifiable minimum.

5.14 The academy will endeavour to carry out its duties in this regard by encouraging an ethos of transparency and openness whilst continuously monitoring efficiency and security by means of appropriate challenge.

6. Definitions

6.1 All of the following (abbreviated) definitions are of relevance to the understanding of this policy. A more extensive list of unabridged definitions from GDPR appears in Appendix 2 – some, but by no means all, of the additional terms defined in the appendix may also feature within the text of this policy.

6.2 **Data** means information which is:

- held on computer (or otherwise recorded with the intention that it will be put on computer at a later date)
- contained in a paper-based filing system (or kept in hard copy with the intention that it will be added to such a system at a later date)
- part of an 'accessible record' – this includes education records.

6.3 **Personal data** means any information relating to an identifiable living individual (the **data subject** – defined below).

6.4 **Identifiable** refers to a person who can be identified, directly or indirectly, by reference to information which the data controller holds. Identification may be possible through an identifier (such as a name or an identification number) or may relate to factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. The possibility of such identification will be relevant to much of the personal information held by the academy, whether on computer or in paper files, and the definition of personal data may also, in certain circumstances, be applicable to pseudonymised data.

6.5 Examples of personal data (that from which an individual might readily be identified) which are most likely to be of relevance to schools include the following:

- salary and bank account details of employees held either on computer or in a manual filing system

- an email about an incident which names a member of staff or a pupil (or members of a pupil's family)
- a line manager's records which contain reference to named members of staff
- a line manager's notebook containing information on only one individual, but where there is an intention to put that information on file
- a set of completed application forms
- any other information which is in (or is likely to come into) the possession of the data controller and which includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person, in respect of the individual.

6.6 In terms of data, GDPR further differentiates (as did DPA 1998) between personal data and 'sensitive' (in DPA terminology) personal data (referred to in GDPR as '**special category data**'). In general, organisations require stronger grounds of justification on which to process sensitive (special category) data than they require to process 'regular' (personal) data, as such data warrants additional protection.

6.7 Special category (or sensitive) data is defined within GDPR in a broadly similar manner to that previously outlined in DPA 1998. This terminology is specifically applicable to (the processing of) personal data concerning an individual's health (such as details of sickness absence records or occupational health referrals) or that which reveals (for instance) racial or ethnic origin, sexual orientation or activities, religious or philosophical beliefs, political affiliations or opinions, membership of a trade union, or criminal proceedings or convictions. It also includes the processing of biometric or genetic data (the former being of specific relevance to many schools).

6.8 A **data subject** means a living individual who is the subject of personal data, and who can be identified by means of that data.

6.9 Data **processing** means any operation performed on personal data and this refers to obtaining, recording or holding such information, or carrying out any operation on the data such as using, reviewing, amending or deleting information. In other words, it includes all activities related to data, including storage. **It is the employer's responsibility to identify a lawful basis for processing under GDPR**.

6.10 Every individual school which is regarded as being a public authority (and this will be applicable to all maintained schools and academies) is required under GDPR to appoint a named individual as its **data protection officer** (DPO), whose role (further defined in the following section) is to be responsible for all aspects of data protection within the academy.

6.11 Every public authority is deemed to be its own data controller (so in the case of the academy the data controller is the organisation itself, therefore no individual need be appointed to that position). A **data controller** is authorised to determine, either alone or jointly with others, the purposes and means of processing personal data (as opposed to a data processor, who processes personal data on behalf of a data controller).

6.12 A **data processor**, who is responsible for the actual processing of personal data on behalf of a data controller, is placed under specific legal obligations by GDPR. These include, for example, the requirement to maintain records of personal data and of processing activities.

6.13 A data processor bears legal liability if found to be responsible for a **data breach**, which is defined as a breach of security which has led to the destruction, loss, alteration or unauthorised disclosure of, or access to, personal data.

6.14 A data controller is not relieved of legal obligations under GDPR where a data processor is involved, in that the controller is charged with the responsibility of ensuring that contracts with processors comply with GDPR.

6.15 Under GDPR, personal data can only be lawfully processed under certain legally defined conditions, and to comply with legislation **lawful processing of personal data** will only be recognised in the presence of one of the following circumstances, which must be identified and documented in both the academy's privacy notice and its information asset register.

6.16 To render processing of personal data lawful, such processing must be necessary for one of the following reasons:

i. performance of (or taking steps to engage in) a contract with the data subject

ii. compliance with a legal obligation

iii. performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

iv. protecting the vital interests of a data subject or another person

v. 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)

failing which it can only be lawful if:

vi. the consent of the data subject has been obtained.

6.17 Under GDPR, special category data can only legitimately be processed under certain legally defined conditions. To comply with legislation, **lawful processing of special category data** will only be recognised in the presence of one of the following circumstances, which must be identified and documented both in the academy's privacy notice and in its information asset register.

6.18 To render processing of special category data lawful, it must be necessary for one of the following reasons:

i. where the processing is 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)

ii. where the processing relates to personal data manifestly made public by the data subject

iii. where the processing is necessary for:

a) carrying out obligations under employment, social security or social protection law, or a collective agreement

b) protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

c) the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

d) reasons of substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards

e) legitimate activities of a non-profit making organisation with a political, philosophical or trade union aim …*

f) purposes of preventative or occupational medicine, for assessing the working capacity of the employee …*

g) reasons of public interest in the area of public health …*

h) archiving purposes in the public interest …*

certain of these conditions are relatively unlikely to be of direct relevance to schools and academies and accordingly the circumstances have been abridged for the purposes of this policy

in which event the legal basis for processing must be identified and documented in the school's information asset register prior to any data being processed.

6.19 If none of the above reasons is satisfied, processing of special category data can only be deemed lawful if:

- the explicit consent of the data subject has been obtained; or
- the personal data has manifestly been placed in the public domain by the subject.

6.20 The academy's justification for data processing will be clarified in their privacy notice in addition to being documented within the information asset register (described below). A **privacy notice** (further defined in the relevant section) is a source of information that explains to a data subject how and why a data controller processes an individual's personal data. The privacy notice should be made freely available to the data subject and accordingly the academy's privacy notice will be displayed on its website.

6.21 An **information asset register** (although this term appears not to be defined in GDPR) is simply a coherent record of the personal data which is held by the academy, categorised by a (summarised) description of the various types of information held and the justification for holding such data, and this represents an essential tool in the academy's strategy to evidence compliance with GDPR by documenting how the organisation processes personal data, from collection to disposal.

6.22 In relation to **consent**, in the context of constituting justification for lawful processing of data (as above), GDPR specifies that this will only be valid if it meets the following conditions:

- it must be informed
- it must be freely given
- it must be specific (referring to the purposes and nature of the processing activity)
- it must represent an unambiguous indication of the individual's wishes
- it must be a positive indication and cannot be assumed or inferred (from inaction, silence or a pre-completed tick box)
- any consent obtained **must** be documented (and this must include a record of how and when consent was obtained)
- any consent obtained can be withdrawn by the individual at any time
- in respect of a child under the age of thirteen consent will only be valid if obtained (in accordance with the above conditions) from a parent or carer (other than when the processing relates to preventative or counselling services offered directly to a child).

6.23 An additional responsibility under GDPR is placed on employers with more than 250 employees (this will not be relevant to the vast majority of schools) who must keep clear

and easily accessible records of high-risk processing (that of special category or sensitive personal data).

6.24 The specific requirements of the records to be kept by employers with more than 250 employees depend on whether the business is a data controller (applicable to schools) or a data processor. These records held must be kept in writing (including electronically) and made available on request to a supervisory authority (which in the UK is the Information Commissioner's Office). The ICO can demand to see these records at any time and they must be easily accessible.

6.25 GDPR contains further provisions (applicable to all employers) on **automated individual decision-making** (reaching a decision solely on the basis of automated means without any human involvement) and on **profiling** (automated processing of personal data to evaluate certain things about an individual).

6.26 Profiling can be part of an automated decision-making process, and GDPR has additional rules to protect individuals if such practice (used in isolation) has legal or similarly significant effects on those individuals. It is not felt likely that many, if indeed any, schools currently use such methods, but in the event that they are deployed either now or at any time in the future the additional information contained in Appendix 3 may be of value.

7. DPO (Data Protection Officer) role

7.1 As a public authority, every individual school (this is applicable to both maintained schools and academies) is regarded as being its own data controller (so no individual need be appointed to that position). It is, however, required under GDPR to appoint a named individual as **Data Protection Officer** (DPO).

7.2 The academy's DPO is responsible for:

- informing and advising the governing body in relation to all aspects of their responsibilities under GDPR (and other data protection legislation)
- supervising training and CPD to staff members on relevant aspects of data processing and data protection
- maintaining comprehensive records of all data processing activities
- managing internal data protection activities
- monitoring compliance with GDPR (and other data protection legislation) by carrying out appropriate audits and assessments
- being the interface between data subjects and the academy, informing the data subjects of how their data is being used, and their rights in relation to this
- being the first point of contact for regulatory authorities.

7.3 Although each school must appoint a DPO the position can be shared between schools in that the role of DPO in two or more schools can be held by one individual, as long as that person is easily accessible to all constituent schools (such as might be found in a cluster).

7.4 The DPO need not be an external appointment: the role may be suitable for an existing employee, most likely as an additional element to their existing role (**although there must be no conflict of interest with this**) rather than as a discrete stand-alone appointment, but whoever is appointed to the position requires to have appropriate expertise and professional qualities, and should hold sufficient authority to be able to challenge senior management and/or governors in the event that there are differences of opinion in relation

to issues affecting data processing in relation to data protection, storage, retention, communication etc.

7.5 The chosen individual will be appointed to the role of DPO by means of a contractual arrangement ensuring tenure of no less than two (calendar) years, and as from May 2018 this post will be held by Jane Burton.

7.6 Sufficient resources will be made available by the academy to the DPO to enable the appointed individual to fulfil their role by discharging their duties as outlined above.

7.7 The DPO will report to the highest level of management at the academy, which is the Chair of Trustees, but will operate independently of line management and will not be dismissed, disciplined or otherwise subjected to recrimination for performing their role in a diligent manner.

7.8 Schools may elect to clarify the role of the DPO on their website or via other media, and a notice to this effect might be anticipated to make use (either in part or in whole) of the text contained within Appendix 4.

8. Privacy notice

8.1 The essential purpose of a privacy notice is to set out (in the public domain) the nature of the data held by the organisation and the purpose for which such data is collected and maintained. It effectively sets out the organisation's legal right to process data as a necessary element of carrying out its legitimate business. This right can be challenged so the reason(s) quoted must be sufficiently robust as to stand up to scrutiny.

8.2 All information contained within a privacy notice must be concise, intelligible, transparent and easily accessible. It must be written in clear and plain language (and if services are to be offered directly to a child, the privacy notice must be written in a manner that the child will understand).

8.3 The privacy notice must be made readily available and supplied without charge.

8.4 The academy undertakes to comply with all the above points in respect of its privacy notices.

8.5 The academy's privacy notice will clarify (by identifying a relevant justification for processing) that explicit consent is not required by the academy for most categories of data. Any exceptions to this underlying premise will be clearly specified.

8.6 The academy appreciates that occasional processing of special category (sensitive) personal data (such as, for instance, medical details which may be required in connection with occupational health referral) may only be rendered lawful on the basis of explicit consent having been obtained (in full accordance with the principles of GDPR) from the data subject. The academy's privacy notice and information asset register will be annotated to reflect this requirement.

8.7 In relation to personal data obtained, the following information will be supplied within the privacy notice:

- the rights of the data subject (including the right to withdraw consent at any time and to lodge a complaint with a supervisory authority)
- the identity and contact details of the data controller

(*for the purposes of GDPR the academy is a public authority and is thus its own data controller; the academy is also regarded (under GDPR) as the legal employer, irrespective of its position in relation to the local authority*)

- details (including contact details) of the data protection officer (DPO)
- the purpose and legal basis (including an indication of legitimate interest) for processing the data
- the data controller's source of the personal data, if it has not been provided directly by the data subject
- the consequences for the employee, where a statutory or contractual requirement exists for the data subject to provide specific data, of failure to comply with this requirement
- details of recipients, or categories of recipients, of the data (if applicable)
- details of any automated decision-making process such as profiling (if applicable)
- an indication of whether the personal data is processed outside the European Economic Area (EEA) and, if so, what protections are in place to safeguard the personal data
- details of how long the data will be retained (and, if no time frame can be provided, how the retention period will be calculated).

8.8 Privacy notices will be available online via the academy's website and will also be provided as required to employees and to pupils (and/or their parents/carers) at the time they engage with the organisation.

8.9 It is good practice to deliver privacy notices via the (same) medium which has been used to collect the personal information. If information has been collected by means of an online form it is appropriate to signpost the privacy notice at the same time via this medium. If, however, the information has been collected on paper it would be appropriate to issue (or at least draw attention to) the privacy notice on hard copy, once again at the same time as the information is collected.

8.10 It may be appropriate to use a graduated approach to information provision by making key privacy details freely available but reserving more detailed information for those who wish to see it. This approach may be helpful when there is insufficient space in which to provide full detail or if a particularly complex explanation is required.

8.11 Where data is obtained directly from the data subject, relevant information in respect of whether the provision of personal data is part of a statutory or contractual requirement (as well as any possible consequences of failing to provide such personal data) will be supplied to the individual at the time the data is obtained.

8.12 Where data is not obtained directly from the data subject, relevant information in respect of the categories of personal data that the academy holds, and the source(s) from which the personal data originates (including whether this came from publicly accessible sources), will be supplied to the individual within one month of the data having been obtained. However, in the event of disclosure to another recipient being envisaged, the above information must be supplied before the data is disclosed, or in cases where the data is used to communicate with the individual it must be supplied no later than the time at which the first such communication takes place.

9. Impact assessments

9.1 To exemplify accordance with GDPR (including the concepts of privacy by design and privacy by default) the academy (guided by the DPO) will implement technical and organisational measures to demonstrate that appropriate consideration has been afforded to data protection and security and that best practice has been embedded into its data processing activities.

9.2 Data protection impact assessments (DPIAs) will be undertaken (under DPA 1998 these may previously have been referred to as privacy impact assessments or PIAs) to assist compliance with the academy's obligations in relation to data protection.

9.3 All contractors, consultants, partners or other agents of the academy who may have access to personal data processed by the organisation must undertake to allow (if requested) data protection audits or DPIAs by the academy of any such data that may be held on the organisation's behalf.

9.4 DPIAs will be carried out at the time of introduction of technological advances to safeguard the rights and freedoms of individuals (in accordance with the concepts of privacy by design and privacy by default) and to identify any potential issues in a pre-emptive manner.

9.5 The academy is conscious that certain processing activities involve relatively high risk, and particular diligence will be taken in respect of such activities.

9.6 These processing activities include (but are by no means limited to) the following:

- special category data in relation to health
- special category data in relation to criminal convictions
- use of CCTV
- use of biometric data
- profiling

although not all these categories are necessarily of current relevance to the academy (or indeed anticipated to become relevant in the foreseeable future).

9.7 Each individual DPIA will include the following information:

- a comprehensible description of the relevant processing operation and its purpose (including an assessment of the justification and proportionality of the processing)
- an outline of the perceived risks (in terms of data protection) to individuals
- a description of the measures put in place to address these risks.

9.8 In the event that a DPIA indicates that the risks may be disproportionate to the anticipated benefits gained from the (extant or proposed) processing activity the academy may consult the Information Commissioner's Office (ICO) to seek its opinion and advice as to whether such processing complies with GDPR.

10. CCTV

10.1 Personal data refers to any data from which a specific individual can be identified. The definition of personal data is not limited to written information and will include such activities as CCTV and employee monitoring, which will typically be considered high-risk activities under GDPR.

10.2 Photography (which term is inclusive of CCTV) is covered in greater detail within the academy's Code of Safe Working Practice (with which the following text is compatible) but the topic is included here to expressly remind all parties (as this point is open to misinterpretation) that such imagery will constitute **personal data** in all cases where the subject is identifiable from the images held.

10.3 The academy appreciates and acknowledges that recording images of identifiable individuals therefore equates to processing personal information and undertakes to conduct such practice (as and when applicable) in accordance with data protection principles. CCTV recordings and other related data must therefore be stored securely and encrypted wherever possible.

10.4 Accordingly, the academy will notify all pupils, staff and visitors of the purpose for collecting CCTV images via our privacy notices, and similarly undertakes only to place CCTV cameras in locations where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

10.5 CCTV footage will be kept in accordance with the retention schedule. Whilst such material is retained, the Chief Operating Officer is responsible for keeping the records secure and allowing access to officially authorised persons.

10.6 The academy will always notify concerned parties of its purpose in taking photographs of pupils and will seek appropriate consent before publishing them, and in the event of the academy desiring to use such imagery (whether still photos or video) in a publication, such as the school website or prospectus or in an advertisement for a staff vacancy, written permission for the specific usage will be sought from either the parent of the pupil (if the pupil is under 13 years of age) or from the pupil themself.

11. Data security

11.1 In terms of data security, **all personal data** (not just special category/sensitive data) **is to be considered confidential material**.

11.2 In relation to manual (paper) records, confidential material must not be left unattended and must be stored in a secure (lockable) filing cabinet, drawer or safe, with access restricted to persons with appropriate authorisation. Similarly, all computers (and other electronic devices) on which confidential material could potentially be accessed must never be left unattended with an unlocked screen.

11.3 In relation to digital (electronic) records, all confidential material stored on-site will be backed up regularly and saved off-site. In this regard devices such as portable hard drives, flash drives and other hardware utilising USB interface will not be used to hold or transfer personal information unless they are password protected and fully encrypted.

11.4 All computing equipment, including portable computing equipment such as laptops, must be password protected and, where possible, encrypted to safeguard against unauthorised access.

11.5 All employees will receive training in respect of the use of passwords: these should be sufficiently robust to ensure that they are not easily compromised and should in any case be subject to periodic alteration for security purposes.

11.6 Members of staff (and governors) must not store, by downloading or saving to their own personal computers, laptops or devices (including mobile phones and smartphones etc) or

by using personal cloud storage systems (such as Dropbox etc) any personal data for which the academy is the data controller.

11.7 In the event that any confidential material is taken off school premises, whether in electronic or hard copy format, staff will take extra care to follow the same procedures for security by keeping devices and documentation under lock and key.

11.8 No electronic data should be taken off premises unless the device it is stored upon is password protected and encrypted.

11.9 In the event of information being taken from the school premises (by whatever means) the individual taking the information will be held responsible for the security of the data.

11.10 Emails containing confidential data must be protected using the academy's secure email system.

11.11 Care will be taken to ensure that any generic communication circulated to parents (of more than one pupil) is sent blind carbon copy (bcc) in order that personal email addresses are not divulged to other recipients.

11.12 Similarly, care will always be taken to ensure that confidential information despatched by any means (whether electronic or hard copy) can only be received by the intended recipient.

11.13 Before sharing (in accordance with their role) any confidential data with authorised persons all members of staff will ensure the following:

- that they are permitted to share the data
- that adequate security is in place to protect the data
- that the requirement for sharing the data with such an individual or company has been evidenced in a privacy notice.

11.14 Visitors to the academy are not permitted access to confidential data and any visitors who are allowed access to areas of the school containing such information are required to be supervised throughout.

11.15 All contractors, consultants, partners or other agents or associates of the academy must be aware that any breach of any provision of GDPR for which they are held responsible will be deemed as being a breach of any contract between the academy and that individual, organisation or company.

11.16 Such parties must also ensure that, should they (or any of their staff) have access to personal data held or processed by, for, or on behalf of, the academy, all such individuals are aware of this policy and are fully trained in their duties and responsibilities under GDPR.

11.17 The physical security of the academy's premises and data storage systems will be subject to review on a regular basis and additional measures put in place as appropriate to reinforce data security.

11.18 The Chief Operating Officer is the individual responsible for ensuring that integrity of the academy's measures to safeguard data confidentiality is maintained.

11.19 The Chief Operating Officer is similarly responsible for ensuring that appropriate continuity and recovery measures are in place in the event of unanticipated system failure (effectively meaning that the academy's disaster recovery plan must include such

measures as may be necessary to ensure security of confidential data is maintained in such circumstances).

11.20 The academy takes its duties under GDPR seriously and any breach of this policy may result in disciplinary action being taken against the individual responsible.

12. Data breaches

12.1 The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration or unauthorised disclosure of, or access to, personal data.

12.2 The Data Protection Officer (DPO) will ensure, as part of training and CPD, that all staff members are made aware of, and understand, what constitutes a data breach.

12.3 In the event of the academy becoming aware of a data breach which is likely to result in a risk to the rights and freedoms of individuals (this to be determined on a case by case basis) the academy will report the circumstances to the Information Commissioner's Office (ICO) within 72 hours of the academy becoming aware of the breach.

12.4 In the event that a breach is likely to result in a high risk to the rights and freedoms of an identified individual the academy will notify the individual concerned directly (note that the definition of a 'high risk' breach necessarily implies that the threshold for notifying the individual is different to that for notifying the relevant supervisory authority).

12.5 In the (albeit rare) event that a breach is deemed to be sufficiently serious, it may be necessary for the public to be notified without undue delay.

12.6 The academy will implement effective and robust procedures to detect, investigate and report (internally) any data breach to assist in reaching a prompt decision as to whether the ICO and the affected individual (or the public) need to be notified.

12.7 In the event of a breach notification being required the following information will be outlined within the notification:

- 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 anticipated (or possible) consequences of the personal data breach (and this may include an indication of whether such consequences are thought to be relatively likely or to be highly improbable)
- a description of the proposed measures to be taken to deal with the personal data breach and (where applicable) a description of the measures taken to mitigate any possible adverse effects.

12.8 Failure to report a breach in the appropriate manner when required to do so may result in an additional fine, further to a fine for the breach itself.

13. Data retention

13.1 Data will not be kept for any longer than is necessary, and this will always be in accordance with the principles of GDPR and the academy's published retention schedule.

13.2 Data which is no longer required will be disposed of in a secure manner as soon as is practicable. Paper documents will be shredded or pulped, and electronic data securely deleted, when there is no longer any justification for their retention.

13.3 Certain educational (or appraisal) records relating to former pupils (or former employees) of the academy may be kept for an extended period not only for legal reasons but also to enable the completion of references or production of evidence on pay progression as well as in relation to academic transcripts or other provision.

14. SARs (Subject Access Requests)

14.1 If the academy receives a written request from a data subject to see any or all personal data that the academy holds about them this should be treated as a subject access request (SAR) (further detailed in Appendix 1 under the 'right of access').

14.2 The academy must respond to this request within the statutory deadline of one month (unless there are extenuating circumstances as specified in Appendix 1).

14.3 If a SAR is submitted in the context of a disciplinary process or potential tribunal claim, the academy will ensure they are fulfilling their data protection obligations while protecting the organisation's business.

14.4 There is no restriction on the number of SARs a data subject can make. Under GDPR (unlike DPA 1998) the first copy of a SAR response must be provided free of charge (although the academy may charge a reasonable fee for additional copies) and the information must be provided in a structured, commonly used and machine-readable format. The academy must ensure that a defined procedure is followed for preparing the response and documenting it.

14.5 An informal request to view, or have copies of, personal data may be dealt with on an informal basis, as and when possible at a mutually convenient time, but in the event of any disagreement over this the person requesting the data will be advised to formalise their application in writing, following which the academy will comply with its duty to respond within the specified time limit.

15. Breach of policy

15.1 Failure to comply with the requirements of this policy could lead to (legal) action being taken against the academy by third parties. Non-compliance is therefore considered to be a serious disciplinary matter which, depending on the circumstances, could potentially lead to sanctions (up to and including dismissal) against the person responsible.

15.2 Staff also require to be aware that an individual employee can commit a criminal offence by, for example, obtaining and/or disclosing personal data for their own purposes without the consent of the data controller.

16. Information Commissioner's Office

16.1 The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness on the part of public bodies and safeguarding data privacy for individuals.

16.2 The ICO maintains a public register of data controllers. Each register entry includes the name and address of the data controller, together with a general description of the processing of personal data carried out.

16.3 Notification is the process by which details of data controllers are added to the register. The Data Protection Act requires every data controller who is processing personal data to notify unless they are exempt.

16.4 The academy is registered with the ICO as a data controller.

16.5 Contact details for the ICO are as follows:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Enquiry/Information Line: 01625 545745

16.6 Further detailed information regarding the register can be found at http://www.ico.gov.uk/.

17. Other policies and procedures

17.1 This policy will be supported by the following policies and procedures:

- Code of Safe Working Practice

Appendix 1: Rights conferred by GDPR

Under **the right to be informed** the following will apply:

1. Privacy notices will be supplied to staff and pupils/students (and their parents/carers) at the time they join the school and will also be available online via the school's website.
2. The privacy notice supplied to individuals in respect of the processing of their personal data will be written in clear, plain language which is concise, transparent and easily accessible, and this will be supplied free of charge.
3. In the event that services are offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.
4. In relation to personal data obtained, the following information will be supplied within the privacy notice:
    - the rights of the data subject (including the right to withdraw consent at any time and to lodge a complaint with a supervisory authority)
    - the identity and contact details of the employer as data controller
    - details of the data protection officer (where the organisation has one)
    - the purpose and legal basis (including an indication of legitimate interest) for processing the data
    - the data controller's source of the personal data, if it has not been provided directly by the data subject
    - the consequences, where there is a statutory or contractual requirement for the data subject to provide data, of failure to do so
    - recipients, or categories of recipients, of the data (if applicable)
    - details of any automated decision-making process such as profiling (if applicable)
    - an indication of whether the personal data is processed outside the European Economic Area (EEA) and, if so, what protections are in place to safeguard the personal data
    - details of how long the data will be retained (and, if no time frame can be provided, how the retention period will be calculated).
5. Where data is obtained directly from the data subject, information will be provided in respect of 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, and this information will be supplied at the time the data is obtained.
6. Where data is not obtained directly from the data subject, information will be provided in respect of the categories of personal data that the school holds, the source(s) from which the personal data originates and whether this came from publicly accessible sources, and this information will be supplied.to the individual within one month of having obtained the data, unless disclosure to another recipient is envisaged in which event it must be supplied, at the latest, before the data is disclosed, or in cases where the data is used to communicate with the individual in which event it must be supplied, at the latest, at the time of the first communication taking place.

Under **the right of access** the following will apply:

1. Individuals have the right to obtain confirmation that their data is being processed.
2. Individuals 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.
3. The school will verify the identity of the person making the request before any information is supplied.

4. A copy of the information will be supplied to the individual free of charge; however, the school reserves the right to impose a 'reasonable' fee to comply with requests for further copies of the same information.
5. Where a subject access request (SAR) has been made electronically, the information will be provided in a commonly used electronic format.
6. In the event that a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
7. All fees will be based on the (estimated) administrative cost of providing the information.
8. All requests will be responded to without undue delay (and, at the latest, within one month of receipt).
9. In the event of numerous or complex requests, the period of compliance will be extended by a further period of two months. In these circumstances the individual submitting the request will be informed of this (and will receive an explanation of why the extension is deemed necessary) within one month of the receipt of the request.
10. 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 seek judicial remedy, within one month of such refusal.
11. In the event that a large quantity of information is being processed about an individual, the school may ask the individual making the request to specify which particular information their request relates to.

Under **the right to rectification** the following will apply:

1. Individuals are entitled to have any inaccurate or incomplete personal data corrected and can submit a request for this either verbally or in writing. Managers need to consider how to implement systems to respond and manage correction requests.
2. Where the personal data in question has been disclosed to third parties, the school will inform those third parties of the rectification where possible.
3. Where appropriate, the school will inform the individual about the third parties to whom that data has been disclosed.
4. Requests for rectification will be responded to within one month, although this may be extended by two months where the request for rectification is complex.
5. The school may refuse to comply with rectification if the request is manifestly unfounded or excessive, and in the event of declining to respond on these grounds 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 seek judicial remedy.

Under **the right to erasure** the following will apply:

1. Individuals are entitled to request the deletion or removal of personal data where there is no compelling reason for its continued processing and can submit a request for this either verbally or in writing.
2. Individuals 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 or processed
    - the individual withdraws their consent, and that consent was the only legal basis for the continued processing of that data

- 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 to comply with a legal obligation
- the personal data is processed in relation to the offer of information society services to a child

3. The right to erasure does not apply if processing is necessary in connection with the exercise of freedom of expression and information or to comply with a legal obligation or for other (specified) purposes in the public interest.
4. Different regulations are applicable in respect of the processing of data which has been collected on the basis of consent obtained from a child (as they may not fully understand the implications or risks involved in the processing of data at the time when consent is obtained) and special attention must be taken in the event of a subsequent request for erasure of such data, irrespective of their age at the time of the request.
5. 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.
6. 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.

Under **the right to restrict processing** the following will apply:

1. This right gives an individual an alternative to requiring data to be erased: effectively it allows the individual to require data to be held in limbo whilst other challenges are resolved.
2. If processing of personal data is 'restricted', then the controller may only store the data. The data may not be further processed unless the individual consents; or the processing is necessary for establishment etc of legal claims; for the protection of the rights of another person; or for reasons of important public interest.
3. Data processing may be restricted in the following circumstances:
    - where the individual disputes the accuracy of data (in which event personal data will be restricted pending verification of the disputed element)
    - where the individual objects to processing (on the basis that the justification for this is not legitimate) (in which event the personal data will be restricted pending consideration and determination of legitimacy)
    - where the processing is deemed to be unlawful but the individual objects to erasure and requests restriction instead
    - where the controller has no further requirement (or justification) for the data but the individual requires the personal data to establish, exercise, or defend legal claims.
4. If the data in question has been disclosed to others, then the controller must (unless this is impossible or involves disproportionate effort) notify those recipients about the restricted processing.
5. The school will inform individuals when a restriction on processing has been lifted.

Under **the right to data portability** the following will apply:

1. This right affords the individual greater control, and an increased level of choice, over the data that controllers hold. Data subjects are entitled to reuse their personal data for their own purposes

across different services and should thus be able to move between service providers without any loss of data thereby enjoying a seamless transition that avoids the data subject having to repeat the task of inputting any information.

2. This right is applicable to personal data that an individual has provided to a data controller in circumstances where the processing is based on either the individual's consent or for the performance of a contract and where the processing is carried out by automated means
3. To comply with this right, it is necessary for the school to provide the personal data in a structured, commonly used and 'machine readable' form. Machine readable means that the information is structured so that software can extract specific elements of the data, enabling other organisations to use the same data.
4. Such data must be provided and transferred free of charge.
5. If the individual requests it, the school may be required to transmit the data directly to another organisation if this is technically feasible. However, the school is not required to adopt or maintain processing systems that are technically compatible with other organisations. There is no charge for this request.
6. In the event that the personal data concerns more than one individual, the school must consider whether providing the information would prejudice the rights of any other individual.
7. The school will respond without undue delay, and within one month, but where the request is complex this can be extended to two months and this must be explained to the individual within one month of receipt of the request.
8. 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 receipt of the request.
9. Where no action is being taken in response to a request, the school will, without undue 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 seek a judicial remedy.

Under **the right to object** the following will apply:

1. The school will inform individuals 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.
2. Individuals have the right to object to the following:
    - processing based on legitimate interests or the performance of a task in the public interest
    - direct marketing
    - processing for purposes of scientific or historical research and statistics.
3. Where personal data is processed for the performance of a legal task or legitimate interests:
    - an individual's grounds for objecting must relate to their 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 the school can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual.
4. Where personal data is processed for direct marketing purposes:
    - 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.

5. 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.
6. Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

Appendix 2: Definitions contained within GDPR

1. **Personal data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
2. **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
3. **Restriction of processing** means the marking of stored personal data with the aim of limiting their processing in the future
4. **Profiling** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements
5. **Pseudonymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person
6. **Filing system** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis
7. **Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
8. **Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
9. **Recipient** means a natural or legal person, public authority, agency or another body, to which the personal data is disclosed, whether a third party or not
10. **Third party** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data
11. **Consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which that person, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them
12. **Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
13. **Genetic data** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question
14. **Biometric data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm

the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data

15. **Data concerning health** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about their health status

Appendix 3: Automated decision making and profiling

The GDPR restricts organisations from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals.

For something to be solely automated there must be no human involvement in the decision-making process. Individuals have the right not to be subject to a decision which is based on automated processing (e.g. profiling) or a method which produces a legal effect (or a similarly significant effect) on the individual.

The school may not currently use such methods, but in the event that they are deployed at any time in the future the school undertakes to ensure that individuals are able to obtain human intervention in order to express their point of view and to obtain an explanation of the decision and challenge it should they wish to do so.

As and when automatically processing personal data for profiling purposes, the school will ensure that appropriate safeguards are in place, and these will include:

- 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.

Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- the school has the explicit consent of the individual
- the processing is necessary for reasons of substantial public interest on a legal basis.

Appendix 4: Guide to the role of DPO

The Data Protection Officer (DPO) is tasked with:

i. informing and advising the governing body in relation to all aspects of their responsibilities under GDPR (and other data protection legislation)
ii. monitoring compliance with the General Data Protection Regulation (GDPR) and other data protection laws
iii. monitoring compliance with the organisation's data protection policies
iv. raising awareness of data protection issues
v. providing training and CPD to staff members on relevant aspects of data processing and data protection
vi. maintaining comprehensive records of all data processing activities
vii. managing internal data protection activities
viii. carrying out audits
ix. being the interface between data subjects and the school, informing them of how their data is being used, and their rights in relation to this

In the performance of their tasks, the school's DPO will always be conscious of the need to have due regard to the risk associated with data processing operations and will take into account the nature, scope, context and purposes of all forms of data processing.

The school will take account of the DPO's advice and the information they provide on the school's data protection obligations.

When carrying out a Data Protection Impact Assessment (DPIA) the school will seek the advice of the DPO who will also monitor the process.

The school's DPO acts as a contact point for school employees, for pupils (and their parents/carers) and for the Information Commissioner's Office (ICO). The DPO co-operates with the ICO and will consult as necessary on any matter of relevance.

Accessibility of the DPO:

The school's DPO is easily accessible as a point of contact for:

i. employees
ii. pupils and their parents/carers
iii. the ICO.

The school has published the contact details of the DPO and has communicated these to the ICO.

Appendix 5: SAR form

Subject Access Request Form

1. *Your details (block capitals please)

Surname:	First names:
Title:	Any other names used: (such as maiden name)
Date of birth:	
Current address: Postcode:	Previous address: Postcode:
Telephone number:	
Email address:	

**you will be asked to provide proof of your identity and address – please see the guidance notes attached.*

2. Whose information are you requesting? (please tick relevant box)

- **My own** ☐
- **Someone else's** ☐
- **Both my own and someone else's** ☐

3. *If you are requesting someone else's information, to whom does it relate?

(please provide their details)

**you will be asked to provide proof of entitlement to request information on someone else's behalf.*

Surname:	First names:
Title:	Any other names used: (such as maiden name)
Date of birth:	
Current address: Postcode:	Previous address: Postcode:
Telephone number:	
Email address:	

Your relationship to this person (please tick the relevant box)

- Mother ☐
- Father ☐
- Carer ☐
- Other (please explain below) ☐

Please see the guidance notes attached.

4. Details of the information you are requesting

Please describe the type of information you want to see:
Which people do you think hold the information you are requesting?

5. Proof of identification and entitlement

Documents provided as proof of identity (please see the guidance notes):

- Passport or photo ID driving licence ☐
- Birth certificate ☐
- Bank statement ☐
- Recent utility bill (original, less than 3 months old) ☐
- Change of name documents (original) ☐

Signature of applicant:	Date:

Appendix 6: SAR guidance notes

1. **Personal details:** Please complete your personal details as requested. Please tell us if you have been known by any other name and if you have lived at your previous address for less than two years please provide your previous address. If you are requesting historical information, then provide as many details as possible, for example previous addresses with dates. Use a separate sheet of paper if required.

2. **Details of the information you require:** You should give as much detail as possible about the information you want us to provide and the people you think might hold the information to assist us in our data search.

3. **Proof of identification:** Proof of name and address is required to ensure we only give information to the correct person. We require two original pieces of documentation, e.g. a recent utility bill (less than three months old) or a bank statement showing your name *and* address and an original piece of photo documentation such as a passport or photo ID driving licence. If you have changed your name please provide proof of this. All documents must be originals, photocopies will not be accepted.

4. **Keep your documents secure:** Documents may be brought into school or sent to us in the post. Always send these important original documents by recorded, special or registered delivery/post. The school cannot be held liable for any documents lost in the post.

5. **Proof of entitlement**: Under DPA/GDPR only the data subject has the right to ask to see their own records. All individuals aged 16 or over should make their own subject access requests if they have the mental capacity to make their own decisions (in this context mental capacity is defined as in the Mental Capacity Act 2005) unless they appoint someone else to make the request on their behalf.

6. **Making a request on behalf of someone else:** People making subject access requests on behalf of someone else need to demonstrate that they have the right to do so and we have listed the categories and proof required below.

   *****_please note that if you make a subject access request on behalf of a child or young person aged 12 to 15 years old, we may independently seek their consent to release the documents to you, even if you have parental responsibility for them – this means we may not disclose the information to you if they refuse their consent_.

7. A birth parent making a subject access request on behalf of their child aged below 16 years:

- **Birth mother:** Child's birth certificate.

- **Birth father (married to the birth mother of the child):** Child's birth certificate **and** birth parents' marriage certificate.

- **Birth father (unmarried to the birth mother of the child) for children born before 1 December 2003:** Child's birth certificate showing registration or re-registration of the birth after 1 December 2003 naming the birth father as the child's father **or** Parental Responsibility Order granted by Court **or** Residence Order granted by Court **or** proof of being appointed the child's Guardian by Court, by child's birth mother or other Guardian **or** Parental Responsibility Agreement with the birth mother.

- **Birth father (unmarried to the birth mother of the child) for children born after 1 December 2003:** Child's birth certificate naming the birth father **or** Parental Responsibility Order granted by Court **or** Residence Order granted by Court **or** proof of being appointed the child's Guardian by Court, by child's birth mother or other Guardian **or** Parental Responsibility Agreement with the birth mother.

8. An adoptive parent making a subject access request on behalf of their child aged below 16 years:

- The Adoption Order

9. A person who is not the child's parent making a subject access request on behalf of their child aged below 16 years:

- Residence Order granted by the Court **or**

- Special Guardianship Order granted by the Court **or**

- Proof of permission to make the subject access request, a signed letter or consent form from a person with parental responsibility and/or the child if the child is 12 years or older

10. A person making a subject access request on behalf of a person aged 16 years or over:

- We require proof of permission to make the request on their behalf, such as a signed letter or consent form from the person. We may contact the person for confirmation that we can release the information to you.

11. A person making a subject access request on behalf of a person lacking mental capacity aged 16 years or over:

- For a young person aged 16 – 17 years old we require proof of parental responsibility, as specified in sections 7 and 8 above, or if you are a carer as in section 9 above we require a Residence Order granted by the Court or a Special Guardianship Order granted by the Court.

- For persons aged 18 or over we require proof of a valid Lasting Power of Attorney **or** an Enduring Power of Attorney **or** proof of a Court appointed Deputyship.

Appendix 7: Retention periods recommended by The Information Commissioner's Office

Type of Document	Retention Period
Application form	Duration of employment
References received	1 year
Payroll and tax information	6 years
Sickness records	3 years
Annual leave records	2 years
Unpaid leave/special leave records	3 years
Annual appraisal/assessment records	5 years
Records relating to promotion, transfer, training, disciplinary matters	1 year from end of employment
References given/information to enable references to be provided	5 years from reference/end of employment
Summary of record of service, for example name, position held, dates of employment	10 years from end of employment
Records relating to accident or injury at work	12 years