Combined Data Protection and Freedom of Information Policy

Date of last review:	31 May 2018	**Review period:**	2 years
Date of next review:	31 May 2020	**Owner:**	Data Protection Officer

TABLE OF CONTENTS

Page

PART 1 – DATA PROTECTION

PART 2 – FREEDOM OF INFORMATION

SACKS MORASHA JEWISH PRIMARY SCHOOL

COMBINED DATA PROTECTION AND FREEDOM OF INFORMATION POLICY

PART 1

DATA PROTECTION

1. INTRODUCTION

1.1 Sacks Morasha Jewish Primary School ("**we**" or the "**School**") collects and uses certain types of personal information about staff, pupils, parents and other individuals ("**individuals**" or "**data subjects**") who come into contact with the School in order provide education and associated functions. The School may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation and other related legislation.

1.2 The EU General Data Protection Regulation and the Data Protection Act 2018 (collectively, the "**Data Protection Rules**") applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (*e.g.*, one could use the individual's name to find such individual's information), and if this is the case, it does not matter whether the information is located in a different physical location.

1.3 This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed every [2] years.

2. PERSONAL DATA

2.1 Personal data ("**Personal Data**") is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain. For purposes of these policies, we do not include in the definition of Personal Data any information that a pupil or such pupil's parent or caretaker provides to a third party directly.

2.2 A sub-set of Personal Data, sometimes known as 'sensitive personal data' or 'special category personal data' ("**Sensitive Data**"), is information that reveals:

(a) race or ethnic origin;

(b) political opinions;

(c) religious or philosophical beliefs;

(d) trade union membership;

(e) physical or mental health;

(f) an individual's sex life or sexual orientation; or

(g) genetic or biometric data for the purpose of uniquely identifying a natural person.

3. THE DATA PROTECTION PRINCIPLES

3.1 The six data protection principles as laid down in the Data Protection Rules are to be followed at all times:

(a) Personal Data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions set out in paragraph 4 below are met;

(b) Personal Data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;

(c) Personal Data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;

(d) Personal Data shall be accurate and, where necessary, kept up to date;

(e) Personal Data processed for any purpose(s) shall not be kept in a form which permits identification of individuals for longer than is necessary for that purpose / those purposes;

(f) Personal Data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3.2 The School is committed to complying with the principles in paragraph 3.1 at all times. This means that the School will:

(a) inform individuals about how and why we process their Personal Data through the privacy notices we issue;

(b) be responsible for checking the quality and accuracy of the information;

(c) regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the School's records retention policy;

(d) ensure that when information is authorised for disposal it is done appropriately;

(e) ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;

(f) share personal information with others only when it is necessary and legally appropriate to do so;

(g) set out clear procedures for responding to requests for access to personal information known as subject access requests;

(h) report any breaches of the Data Protection Rules in accordance with the procedure in paragraph 13 below.

3.3 The School does not intend to seek or hold Sensitive Data about staff or students except where the School has been notified of the information, or it comes to the School's attention via

legitimate means (*e.g.*, a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or students are under no obligation to disclose to the School their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, *e.g.*, pension entitlements).

3.4 In addition to the principles set out in paragraphs 3.1, 3.3 and 3.2, the School is committed to ensuring that, at all times, anyone dealing with Personal Data shall be mindful of the individual's rights under the law (as set out in further detail herein).

3.5 Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

4. GROUNDS FOR PROCESSING UNDER THE FIRST DATA PROTECTION PRINCIPLE

4.1 Under the first data protection principle set out paragraph 3.1(a) above, the School will process Personal Data only where at least one of the following applies:

(a) the data subject has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given;

(b) the processing is necessary for the performance of a contract, to which the data subject is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the data subject, at their request;

(c) the processing is necessary for the performance of a legal obligation to which we are subject;

(d) the processing is necessary to protect the vital interests of the data subject or another;

(e) the processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us; or

(f) the processing is necessary for a legitimate interest of the School or that of a third party, except where this interest is overridden by the rights and freedoms of the data subject concerned.

4.2 Under the first data protection principle set out paragraph 3.1(a) above, the School will process Sensitive Data only where at least one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the School or of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing relates to personal data which are manifestly made public by the data subject;

(e) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or

(f) processing is necessary for reasons of substantial public interest, on the basis of applicable law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5. USE OF PERSONAL DATA BY THE SCHOOL

5.1 The School holds and processes personal data on pupils, staff and other individuals such as visitors. In each case, the personal data must be held and processed in accordance with the data protection principles as outlined in paragraph 3.1 above and in this paragraph 4.2 below.

Pupils

5.2 The personal data held regarding pupils will include (without limitation) contact details, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.

5.3 The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the School as a whole is doing, together with any other uses normally associated with this provision in a school environment.

5.4 The School may make use of limited personal data (such as contact details) relating to pupils, and their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the School, but only where consent has been provided for such a use.

5.5 In particular, the School may:

(a) transfer information to any association society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to the School but only where consent has been obtained first;

(b) make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities;

(c) keep the pupil's previous school informed of his / her academic progress and achievements e.g. sending a copy of the school reports for the pupil's first year at the School to their previous school; and

(d) use photographs of pupils in accordance with the photograph policy.

5.6 Any wish to limit or object to any use of personal data should be notified to the Data Protection Officer in writing, which notice will be acknowledged by the School in writing. If, in the view of the Data Protection Officer, the objection cannot be maintained, the data subject will be given written reasons why the School cannot comply with the request.

Staff

5.7 The personal data held about staff will include (without limitation) contact details, employment history, information relating to career progression, information relating to DBS checks, photographs, occupational pensions, and payroll.

5.8 The data is used to comply with legal obligations placed on the School in relation to employment, and the education of children in a school environment. The School may pass

information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

5.9 Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

5.10 Any wish to limit or object to the uses to which personal data is to be put should be notified to the Data Protection Officer who will ensure that this is recorded, and adhered to if appropriate. If the Data Protection Officer is of the view that it is not appropriate to limit the use of personal data in the way specified, the data subject will be given written reasons why the School cannot comply with their request.

5.11 DBS checks are carried out on the basis of the School's legal obligations in relation to the safer recruitment of Staff as stipulated in the Independent School Standards Regulations and the DBS information (which will include personal data relating to criminal convictions and offences) is further processed in the substantial public interest, with the objective of safeguarding children. Retention of the information is covered by the School's records retention policy. Access to the DBS information is restricted to those staff who have a genuine need to have access to it for their job roles. In addition to the provisions of the Data Protection Rules and the Data Protection Act 2018, disclosure of this information is restricted by section 124 of the Police Act 1997 and disclosure to third parties will only be made if it is determined to be lawful.

Other Individuals

5.12 The School may hold personal information in relation to other individuals who have contact with the school, such as volunteers, visitors and guests. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary.

6. INFORMATION ASSET REGISTER

The School will create and maintain an Information Asset Register ("**IAR**") to identify the personal information it holds. The IAR will identify, among other matters, the following information:

(a) the name or description of the type of information

(b) the activity status regarding the information (ceased, ongoing, future)

(c) whether the information is personal information and also if it is sensitive personal information

(d) the School's purpose for holding the information

(e) whether consent has been sought and obtained in accordance with the requirements of the Data Protection Rules

(f) if the information is sensitive information, the special conditions relating to the School's processing of such information

(g) the name of the provider of such information

(h) whether the information is in the public domain, and if so where is it publicly available

(i) who the information will be shared with and accessed by

(j) any special time limits for processing the information

7. SECURITY OF PERSONAL DATA

7.1 The School will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

7.2 The School will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the Data Protection Rules.

8. DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

8.1 The following list includes some of the usual reasons that the School will authorise disclosure of personal data to a third party:

(a) To give a confidential reference relating to a current or former employee, volunteer or pupil;

(b) for the prevention or detection of crime;

(c) for the assessment of any tax or duty;

(d) where it is necessary to exercise a right or obligation conferred or imposed by law upon the School (other than an obligation imposed by contract), including the obligation to provide education to pupils;

(e) for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

(f) for the purpose of obtaining legal advice;

(g) for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);

(h) to publish the results of public examinations or other achievements of pupils of the School;

(i) to disclose details of a pupil's medical condition where it is in the pupil's interests to do so and there is a legal basis for doing so, for example for medical advice, insurance purposes or to organisers of school trips (legal basis will vary in each case, but will usually be based on the vital interests of the pupil, reasons of substantial public interest (for example, safeguarding the pupil or others), or explicit consent);

(j) to provide information to another educational establishment to which a pupil is transferring;

(k) to provide information to the examination authority as part of the examination process (which may in turn pass information to the Department for Education); and

(l) to provide information to each relevant local and national governmental department and/or authority concerned with education or with the operation of the School, including

(i) the Local Authority of Barnet, and

(ii) the Department for Education ("**DfE**").

8.2 The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

8.3 The School may receive requests from third parties (i.e. those other than the data subject, the School, and employees of the School) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies and there is a need to do so; or where necessary for the legitimate interests of the data subject or the School.

8.4 All requests for the disclosure of personal data must be sent to the Data Protection Officer, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

9. CONFIDENTIALITY OF PUPIL CONCERNS

9.1 Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the School will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the School believes disclosure will be in the best interests of the pupil or other pupils. Disclosure for a safeguarding purpose will be lawful because it will be in the substantial public interest.

9.2 A further description of the School's safeguarding policies are available here.

10. SUBJECT ACCESS REQUESTS

10.1 Anybody who makes a request to see any personal information held about them by the School is making a subject access request. All information relating to the data subject, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system" (see paragraph 1.2 above).

10.2 The individual's full subject access right is to know;

(a) whether personal data about him or her are being processed;

(b) the purposes of the processing;

(c) the categories of personal data concerned;

(d) the recipients or categories of recipient to whom their personal data have been or will be disclosed;

(e) the envisaged period for which the data will be stored or where that is not possible, the criteria used to determine how long the data are stored;

(f) the existence of a right to request rectification or erasure of personal data or restriction of processing or to object to the processing;

(g) the right to lodge a complaint with the Information Commissioner's Office;

(h) where the personal data are not collected from the individual, any available information as to their source; and

(i) details of the safeguards in place for any transfers of their data to locations outside the European Economic Area.

10.3 All requests should be sent to the Data Protection Officer within 3 working days of receipt, and must be dealt with in full without delay and at the latest within one month of receipt.

10.4 Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The Data Protection Officer must, however, be satisfied that:

(a) the child or young person lacks sufficient understanding; and

(b) the request made on behalf of the child or young person is in their interests.

10.5 Any data subject, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the School must have written evidence that the data subject has authorised the person to make the application and the Data Protection Officer must be confident of the identity of the data subject making the request and of the authorisation of the data subject to whom the request relates.

10.6 Access to records will be refused in instances where an exemption applies, for example, information sharing may place the data subject at risk of significant harm or jeopardise police investigations into any alleged offence(s).

10.7 A subject access request must be made in writing. The School may ask for any further information reasonably required to locate the information.

10.8 A data subject only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

10.9 All files must be reviewed by the Data Protection Officer before any disclosure takes place. Access will not be granted before this review has taken place.

10.10 Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

10.11 The processing of subject access requests will be free of charge in most cases, other than the right of the School to refuse or charge for requests that are manifestly unfounded or excessive.

11. EXEMPTIONS TO ACCESS BY DATA SUBJECTS

11.1 Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

11.2 There are other exemptions from the right of subject access. If we intend to apply any of them to a request then we will usually explain which exemption is being applied and why.

12. OTHER RIGHTS OF DATA SUBJECTS

12.1 The School has an obligation to comply with the rights of data subjects under the law, and takes these rights seriously. The following section sets out how the School will comply with the rights to:

(a) object to Processing;

(b) rectification;

(c) erasure; and

(d) data Portability.

Right to object to processing

12.2 A data subject has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest (see paragraphs 4.1(e) and 4.1(f) above) where they do not believe that those grounds are adequately established.

12.3 Where such an objection is made, it must be sent to the Data Protection Officer within 3 working days of receipt, and the Data Protection Officer will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the data subjects, or whether the information is required for the establishment, exercise or defence of legal proceedings.

12.4 The Data Protection Officer shall be responsible for notifying the data subject of the outcome of their assessment promptly following the Data Protection Officer's decision concerning the objection (and in any event within any time period required by the Data Protection Rules in that regard).

Right to rectification

12.5 A data subject has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to the Data Protection Officer within 3 working days of receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the data subject notified.

12.6 Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the data subject. The data subject shall be given the option of a review under the data protection complaints procedure, or an appeal direct to the Information Commissioner.

12.7 A data subject also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure

12.8 Data subjects have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

(a) where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;

(b) where consent is withdrawn and there is no other legal basis for the processing;

(c) where an objection has been raised under the right to object, and found to be legitimate;

(d) where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);

(e) where there is a legal obligation on the School to delete.

12.9 The Data Protection Officer will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to restrict processing

12.10 In the following circumstances, processing of a data subject's personal data may be restricted:

(a) where the accuracy of data has been contested, during the period when the School is attempting to verify the accuracy of the data;

(b) where processing has been found to be unlawful, and the data subject has asked that there be a restriction on processing rather than erasure;

(c) where data would normally be deleted, but the data subject has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;

(d) where there has been an objection made under paragraph 12.2 above, pending the outcome of any decision.

Right to portability

12.11 If a data subject wants to send their personal data to another organisation they have a right to request that the School provides their information in a structured, commonly used, and machine readable format. As this right is limited to situations where the School is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be limited. If a request for this is made, it should be forwarded to the Data Protection Officer within 3 working days of receipt, and the Data Protection Officer will review and revert as necessary.

13. BREACH OF ANY REQUIREMENT OF THE DATA PROTECTION RULES

13.1 Any and all breaches of the Data Protection Rules, including a breach of any of the data protection principles shall be reported as soon as it is / they are discovered to the Data Protection Officer.

13.2 Once notified, the Data Protection Officer shall assess:

(a) the extent of the breach;

(b) the risks to the data subjects as a consequence of the breach;

(c) any security measures in place that will protect the information;

(d) any measures that can be taken immediately to mitigate the risk to the data subject.

13.3 Unless the Data Protection Officer concludes that there is unlikely to be any risk to any data subject from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the School, unless a delay can be justified.

13.4 The Information Commissioner shall be told:

(a) the date of the breach;

(b) details of the breach, including the volume of data at risk, and the number and categories of data subjects;

(c) the action taken by the recipient of the data, and the action taken by the School to retrieve such information and respond to the breach;

(d) details of the notification given to the relevant data subject regarding the breach;

(e) the contact point for any enquiries (which shall usually be the Data Protection Officer);

(f) the likely consequences of the breach;

(g) when the person or entity causing the breach last had data protection training relevant to such person's responsibilities; and

(h) measures proposed or already taken to address the breach.

13.5 If the breach is likely to result in a high risk to the rights and freedoms of the affected data subjects then the Data Protection Officer shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected data subjects.

13.6 Data subjects shall be told:

(a) the nature of the breach;

(b) who to contact with any questions;

(c) measures taken to mitigate any risks.

13.7 The Data Protection Officer shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the governing board of the School and a decision made about implementation of those recommendations.

14. CONTACT

14.1 If anyone has any concerns or questions in relation to this policy they should contact the Data Protection Officer.

14.2 The core responsibilities of the Data Protection Officer are:

(a) general responsibility for the School's compliance with the Data Protection Rules;

(b) general responsibility for the development and updating of the School's procedures regarding Data Protection Rules compliance;

(c) supporting the School and its teachers and staff in connection with Data Protection Rules compliance; and

(d) working closely with the School and each other controller and processor of the School's personal information.

PART 2

FREEDOM OF INFORMATION

15. INTRODUCTION

15.1 The School is subject to the Freedom of Information Act 2000 (FOI) as a public authority, and as such, must comply with any requests for information in accordance with the principles laid out in the Act.

16. WHAT IS A REQUEST UNDER FOI

16.1 Any request for any information from the School is technically a request under the FOI, whether or not the individual making the request mentions the FOI. However, the ICO has stated that routine requests for information (such as a parent requesting information regarding a student event) can be dealt with outside of the provisions of the Act.

16.2 In all non-routine cases, all requests should be referred in the first instance to the Data Protection Officer, who may allocate another individual to deal with the request. This must be done promptly, and in any event within 3 working days of receiving the request.

16.3 When considering a request under FOI, a release under FOI is treated as release to the general public, and so once it has been released to an individual, anyone can then access it, and access cannot thereafter be restricted (even by marking the information "confidential" or "restricted").

17. TIME LIMIT FOR COMPLIANCE

17.1 The School must respond as soon as possible, and in any event, within 20 working days of the date of receipt of the request. For the School, a "working day" is a school day (one in which pupils are in attendance), subject to an absolute maximum of 60 normal working days (not school days) to respond.

18. PROCEDURE FOR DEALING WITH A REQUEST

18.1 When a request is received that cannot be dealt with by simply providing the information, it should be referred in the first instance to the Data Protection Officer, who may re-allocate to an individual with responsibility for the type of information requested.

18.2 The first stage in responding is to determine whether or not the School "holds" the information requested. The School will hold the information if it exists in computer or paper format. Some requests will require the School to take information from different sources and manipulate it in some way. Where this would take minimal effort, the School is considered to "hold" that information, but if the required manipulation would take a significant amount of time, the requestor should be contacted to explain that the information is not held in the manner requested, and offered the opportunity to refine their request. (For example, a request requiring the School to add up totals in a spread sheet and release the total figures would be information "held" by the School. If the School would have to go through a number of spread sheets and identify individual figures and provide a total, this is likely not to be information "held" by the School, depending on the time involved in extracting the information.)

18.3 The second stage is to decide whether the information can be released, or whether one of the exemptions set out in the Act applies to the information. Common exemptions that might apply include:

(a) Section 40 (1) – the request is for the applicants personal data. This must be dealt with under the subject access regime in the DPA, detailed in paragraph 9 of the DPA policy above;

(b) Section 40 (2) – compliance with the request would involve releasing third party personal data, and this would be in breach of the DPA principles as set out in paragraph 3.1 of the DPA policy above;

(c) Section 41 – information that has been sent to the School (but not the School's own information) which is confidential;

(d) Section 21 – information that is already publicly available, even if payment of a fee is required to access that information;

(e) Section 22 – information that the School intends to publish at a future date;

(f) Section 43 – information that would prejudice the commercial interests of the School and / or a third party;

(g) Section 38 – information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information);

(h) Section 31 – information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras;

(i) Section 36 – information which, in the opinion of the chair of governors of the School, would prejudice the effective conduct of the School. There is a special form for this on the ICO's website to assist with the obtaining of the chair's opinion.

18.4 The sections mentioned in italics above are qualified exemptions. This means that even if the exemption applies to the information, the School will need to carry out a public interest weighting exercise, balancing the public interest in the information being released, as against the public interest in withholding the information.

19. RESPONDING TO A REQUEST

19.1 When responding to a request where the School has withheld some or all of the information, the School must explain why the information has been withheld, quoting the appropriate section number and explaining how the information requested fits within that exemption. If the public interest test has been applied, this also needs to be explained.

19.2 The letter should end by explaining to the requestor how they can complain – either by reference to an internal review by a governor, or by writing to the ICO.

20. CONTACT

20.1 Any questions about this policy should be directed in the first instance to the Data Protection Officer.