1. Statement of Accountability in respect of Data Protection

Your privacy is important to Belmont House School and we appreciate that we are entrusted with the personal information, including sensitive personal information, of our staff, pupils, parents/guardians, guests, and visitors. For the purposes of this accountability statement, personal information means any information that enables us to identify a specific living individual.

We are obligated by legislation and ethical practices to maintain your personal information in strict confidence and to ensure that your personal information is protected by physical, administrative, and technical safeguards. These obligations apply to personal information in all formats, including oral, written, and electronic formats; moreover, these safeguards must protect all manners of handling personal information, including collection, use, disclosure, access, storage, transfer, copying, modification, and disposal.

Belmont House School – its staff, contractors, volunteers, partners and agents – are responsible for ensuring the confidentiality and protection of your personal information in the custody or control of Belmont House School. As part of our obligations and commitment to you, we are required to abide by the **six data protection principles** detailed below that determine how we may collect, process, and treat your personal information:

1) We will only process your personal information lawfully, fairly, and in a transparent manner.
2) When we collect your personal information, we will only use it for a specified and legitimate purpose and not use your personal information in any other manner unless you give us your express consent.
3) We will only ask for the personal information that we need for a specified and legitimate purpose and will not ask for excessive or irrelevant information.
4) We will ensure that the personal information we hold about you is accurate and, where necessary, kept up to date and will take every reasonable step to ensure that personal information which is out of date will be erased or corrected.
5) We will only hold your personal information for no longer than is necessary for the purposes that we have explained to you as part of our privacy policies and in accordance with our data retention policies. When we store your personal information it will be held in accordance with appropriate technical and organisational measures to safeguard your rights and freedoms.

6) We will only process your personal information in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

We understand that these principles are not just guidelines and that, as part of our obligation to keep your personal information safe and secure, we must be able to demonstrate our compliance with these principles. Therefore, as part of our overall accountability to you we have introduced a governance structure aimed at ensuring that there are individuals within our school who are responsible for data privacy, including an accountable management team and management reporting procedures.

We maintain an inventory of where key personal information is stored, including the flow of key personal data through our school including, where necessary, documenting and disclosing transfers of personal information outside of our school and cross-border. This helps us manage our third-party risk and helps us to track the processing of personal information that we may pass to external parties within the United Kingdom, the European Economic Area, and further abroad. As part of this commitment we are undertaking a review of our existing supplier agreements and endeavoured to put in place arrangements to protect your personal information when it is transferred to a supplier. This may, for example, include revising our existing contracts or putting in place data sharing agreements.

We also maintain internal data protection policies that our staff, employees, contractors, volunteers, and partners are required to comply with in addition to our school code of conduct. At the centre of our internal data protection initiatives is the idea that the protection of personal information should be embedded within the fabric and culture of the school and, to this end, we have incorporated or revised a number of our policies. Furthermore, we understand that having these policies in place does not necessarily mean that they are read and understood. Therefore, we maintain a training and awareness program for data protection and all of our staff are required to complete mandatory training on how to handle personal information – this forms part of our induction process and we review and update our staff, contractors, volunteers, partners, and agents on changes to data protection legislation as new guidance is released by the Information Commissioner's Office.

We regularly audit our information management systems, both physical and electronic, in order to assist the school in understanding and managing its information security risk. We apply a *"Privacy by Design"* approach to how we manage the risks around handling personal information and, to that end, we now use a number of tools to help us measure and monitor personal information risk, for example, completing data protection impact assessments and reviewing third-party contracts through a data protection contract risk matrix and checklist. We regularly review our access control policies to ensure that we minimise the amount of personal information that is accessed by our staff, contractors, volunteers, partners, and agents and, where necessary, encrypt personal information and/or segregate particularly sensitive personal information.

We continue to monitor and update our data protection policies in line with changes to legislation, including the most recent changes introduced under the General Data Protection Regulation which takes effect from the 25th of May 2018.

You can find our most recent website privacy, cookie and data retention policies **[HERE]**. Our policies also explain how we respond to requests and complaints about how we collect, process, and manage your personal information and we have endeavoured to make our policies as transparent and reader-friendly as possible. If you have any questions about how we collect, process, and manage your personal information then please do not hesitate to get in touch us at: **Data Protection Team, Belmont House School, Sandringham Avenue, Newton Mearns, Glasgow G77 5DU.**

Yours sincerely,

Melvyn David Shanks
For and on behalf of
Belmont House School

2. Responsibilities

The School is a Data Controller under the terms of current data protection legislation and has a corporate responsibility to implement the provisions of this legislation. The School determines the purposes for which, and the manner in which, personal data is to be processed.

The School must take appropriate measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction, or damage to, personal data (Principle 7)

The School must maintain a general "right of access" by an individual to their own personal data held by the School and must maintain its records in accordance with the regulatory environment.

The Principal will be responsible for:

- Day to day data protection matters and for developing guidance and training for staff on data protection issues
- The maintenance of the School's Notification with the Information Commissioner
- The processing of all Subject Access Requests submitted to the School under current data protection legislation
- The administration of all complaints from, and investigations requested by, the Information Commissioner.

2.1 All members of staff who create, receive or maintain personal data have responsibilities under current data protection legislation. Staff must ensure that any request for personal data they receive is handled in compliance with this Policy. Specifically, members of staff are responsible for:

- Familiarising themselves with this Policy and current data protection legislation guidelines
- Seeking advice when there is uncertainty about the appropriate action to take with respect to the processing of personal data
- Managing documents and records in accordance with School procedures
- Ensuring that any personal data they hold is held securely, that it is accurate and up to date, and that any personal data they hold is not passed to any unauthorised third party.

The welfare of young people and Child Protection policies will take precedence at all times.

2.2 The Head of Junior School and Principal Teachers are responsible for ensuring that their staff are made aware of the existence and content of this Policy.

2.3 Compliance with this Policy is compulsory for all staff employed by the School and any member of staff who fails to comply with this Policy may be subject to disciplinary action.

3. Retention and Disposal of Personal data

3.1 Personal data must not be kept for longer than is necessary based on the purpose for which it was initially collected (Principle 5). To ensure compliance with this Principle, all Staff must follow the relevant records management procedures which sets down recommended retention and disposal schedules. Only in exceptional circumstances, after consultation with senior management, should personal data be kept indefinitely.

3.2 The disposal of any documents containing personal data must only be undertaken according to the School's Confidential Waste Disposal policy.

4. Subject Access Requests

4.1 About these procedures

4.1.1 Data subjects have certain rights in respect of their personal data. When we process data subjects' personal data, we shall respect those rights. These procedures provide a framework for responding to requests to exercise those rights. It is our policy to ensure that requests by data subjects covered by these procedures to exercise their rights in respect of their personal data are handled in accordance with applicable law.

4.1.2 For the purposes of these procedures, "personal data" means any information relating to an identified or identifiable data subject. An identifiable data subject is anyone who can be identified, directly or indirectly, by reference to an identifier, such as a name, identification number or online identifier. "Processing" means any operation or set of operations that is performed on personal data, such as collection, use, storage, dissemination and destruction.

4.1.3 These procedures only apply to data subjects whose personal data we process.

4.2 Responding to requests to access personal data

4.2.1 Data subjects have the right to request access to their personal data processed by us. Such requests are called subject access requests (SARs). When a data subject makes an SAR we shall take the following steps:

(a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met):

(b) confirm the identity of the data subject who is the subject of the personal data. For example, we may request additional information from the data subject to confirm their identity;

(c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held; and

(d) confirm to the data subject whether or not personal data of the data subject making the SAR are being processed.

4.2.2 If personal data of the data subject are being processed, we shall provide the data subject with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (including electronic) means:

(a) the purposes of the processing;

(b) the categories of personal data concerned (for example, contact details, bank account information and details of sales activity);

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients overseas (for example, US-based service providers);

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

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

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

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and

(i) where personal data are transferred outside the EU, details of the appropriate safeguards to protect the personal data.

4.2.3 We shall also, unless there is an exemption (see paragraph 9 below), provide the data subject with a copy of the personal data processed by us in a commonly used electronic form (unless the data subject either did not make the request by electronic means or has specifically requested not to be provided with the copy in electronic form) within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

4.2.4 Before providing the personal data to the data subject making the SAR, we shall review the personal data requested to see if they contain the personal data of other data subjects. If they do, we may redact the personal data of those other data subjects prior to providing the data subject with their personal data, unless those other data subjects have consented to the disclosure of their personal data.

4.2.5 If the SAR is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing the personal data, or refuse to act on the request.

4.2.6 If we are not going to respond to the SAR we shall inform the data subject of the reason(s) for not taking action and of the possibility of lodging a complaint with the ICO.

4.3 Responding to requests to rectify personal data

4.3.1 Data subjects have the right to have their inaccurate personal data rectified. Rectification can include having incomplete personal data completed, for example, by a data subject providing a supplementary statement regarding the data. Where such a request is made, we shall, unless there is an exemption (see paragraph 9 below), rectify the personal data without undue delay.

4.3.2 We shall also communicate the rectification of the personal data to each recipient to whom the personal data have been disclosed (for example, our third party service providers who process the data on our behalf), unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

4.4 Responding to requests for the erasure of personal data

4.4.1 Data subjects have the right, in certain circumstances, to request that we erase their personal data. Where such a request is made, we shall, unless there is an exemption (see paragraph 9 below), erase the personal data without undue delay if:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws their consent to the processing of their personal data and consent was the basis on which the personal data were processed and there is no other legal basis for the processing;

(c) the data subject objects to the processing of their personal data on the basis of our performance of a task carried out in the public interest or in the exercise of official authority vested in us, or on the basis of our legitimate interests which override the data subject's interests or fundamental rights and freedoms, unless we either can show compelling legitimate grounds for the processing which override those interests, rights and freedoms, or we are processing the data for the establishment, exercise or defence of legal claims;

(d) the data subject objects to the processing of their personal data for direct marketing purposes;

(e) the personal data have been unlawfully processed;

(f) the personal data have to be erased for compliance with a legal obligation to which we are subject; or

(g) the personal data have been collected in relation to the offer of e-commerce or other online services.

4.4.2 When a data subject makes a request for erasure in the circumstances set out above, we shall, unless there is an exemption (see paragraph 4.5 and paragraph 9 below), take the following steps:

(a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

(b) confirm the identity of the data subject who is the subject of the personal data. We may request additional information from the data subject to do this;

(c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held and erase such data within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay;

(d) where we have made the personal data public, we must, taking reasonable steps, including technical measures, inform those who are processing the personal data that the data subject has requested the erasure by them of any links to, or copies or replications of, those personal data; and

(e) communicate the erasure of the personal data to each recipient to whom the personal data have been disclosed unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

4.4.3 If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of erasure, or refuse to act on the request.

4.4.4 If we are not going to respond to the request we shall inform the data subject of the reasons for not taking action and of the possibility of lodging a complaint with the ICO.

4.4.5 In addition to the exemptions in paragraph 9 below, we can also refuse to erase the personal data to the extent processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by law and to which we are subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in us;

(c) for reasons of public interest in the area of public health;

(d) for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

4.5 Responding to requests to restrict the processing of personal data

4.5.1 Data subjects have the right, unless there is an exemption (see paragraph 9 below), to restrict the processing of their personal data if:

(a) the data subject contests the accuracy of the personal data, for a period to allow us to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) we no longer need the personal data for the purposes we collected them, but they are required by the data subject for the establishment, exercise or defence of legal claims; and

(d) the data subject has objected to the processing, pending verification of whether we have legitimate grounds to override the data subject's objection.

4.5.2 Where processing has been restricted, we shall only process the personal data (excluding storing them):

(a) with the data subject's consent;

(b) for the establishment, exercise or defence of legal claims;

(c) for the protection of the rights of another person; or

(d) for reasons of important public interest.

4.5.3 Prior to lifting the restriction, we shall inform the data subject of the lifting of the restriction.

4.5.4 We shall communicate the restriction of processing of the personal data to each recipient to whom the personal data have been disclosed, unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

4.6 Responding to requests for the portability of personal data

4.6.1 Data subjects have the right, in certain circumstances, to receive their personal data that they have provided to us in a structured, commonly used and machine-readable format that they can then transmit to another company. Where such a request is made, we shall, unless there is an exemption (see paragraph 9 below), provide the personal data without undue delay if:

(a) the legal basis for the processing of the personal data is consent or pursuant to a contract; and

(b) our processing of those data is automated.

4.6.2 When a data subject makes a request for portability in the circumstances set out above, we shall take the following steps:

(a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

(b) confirm the identity of the data subject who is the subject of the personal data. We may request additional information from the data subject to confirm their identity; and

(c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held and provide the data subject with such data (or, at the data subject's request, transmit the personal data directly to another company, where technically feasible) within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

4.6.3 If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing or transmitting the personal data, or refuse to act on the request.

4.6.4 If we are not going to respond to the request we shall inform the data subject of the reasons for not taking action and of the possibility of lodging a complaint with the ICO.

4.7 Responding to objections to the processing of personal data

4.7.1 Data subjects have the right to object to the processing of their personal data where such processing is on the basis of our performance of a task carried out in the public interest or in the exercise of official authority vested in us, or on the basis of our legitimate interests which override the data subject's interests or fundamental rights and freedoms, unless we either:

(a) can show compelling legitimate grounds for the processing which override those interests, rights and freedoms; or

(b) are processing the personal data for the establishment, exercise or defence of legal claims.

4.7.2 Data subjects also have the right to object to the processing of their personal data for scientific or historical research purposes, or statistical purposes, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

4.7.3 Where such an objection is made, we shall, unless there is an exemption (see paragraph 9 below), no longer process a data subject's personal data.

4.7.4 Where personal data are processed for direct marketing purposes, data subjects have the right to object at any time to the processing of their personal data for such marketing. If a data subject makes such a request, we shall stop processing the personal data for such purposes.

4.8 Responding to requests not to be subject to automated decision-making

4.8.1 Data subjects have the right, in certain circumstances, not to be subject to a decision based solely on the automated processing of their personal data, if such decision produces legal effects concerning them or similarly significantly affects them. Where such a request is made, we shall, unless there is an exemption (see paragraph 9 below), no longer make such a decision unless it:

(a) is necessary for entering into, or the performance of, a contract between us and the data subject;

(b) is authorised by applicable law which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

4.8.2 If the decision falls within paragraph 8.1(a) or paragraph 8.1(c), we shall implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, including the right to obtain human intervention, to express their point of view and to contest the decision.

4.9 Exemptions

4.9.1 Before responding to any request we shall check whether there are any exemptions that apply to the personal data that are the subject of the request. Exemptions may apply where it is necessary and proportionate not to comply with the requests described above to safeguard:

(a) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; and

(b) the protection of the data subject or the rights and freedoms of others.

5. Complaints

Members of staff must promptly forward to the Principal any comments or complaints about, or omissions from, the School's Notification with the Information Commissioner. Any complaints regarding the processing of personal data by the School will be dealt with in accordance with the School's Complaints Procedures.

Appendix 1: Requests for information about children

Even if a child is too young to understand the implications of subject access rights, data about them is still their personal data and does not belong to anyone else, such as a parent or carer. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.
Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their

rights, then you should respond to the child rather than the parent. What matters is that the child is able to understand (in broad terms) what it means to make a SAR and how to interpret the information they receive as a result of doing so.

When considering borderline cases, you should take into account, among other things:

- the child's level of maturity and their ability to make decisions like this
- the nature of the personal data
- any court orders relating to parental access or responsibility that may apply
- any duty of confidence owed to the child or young person
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment
- any detriment to the child or young person if individuals with parental responsibility cannot access this information
- any views the child or young person has on whether their parents should have access to information about them.

In Scotland, the law presumes that a child aged 12 years or more has the capacity to make a SAR. It does not follow that, just because a child has capacity to make a SAR, they also have capacity to consent to sharing their personal data with others – as they may still not fully understand the implications of doing so.