Stormont School

32a DATA PROTECTION POLICY AND PRIVACY NOTICE

Last reviewed Summer 2021

Next review due Summer 2022

Reviwed by Headteacher

The policy will be published on the website for current and prospective parents, governors, staff and volunteers.
Hard copies are available from the School Office.

BACKGROUND

Data protection is an important legal compliance issue for Stormont School. During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, its contractors and other third parties (in a manner more fully detailed in the School's Privacy Notice – see Annex A). The School, as "data controller", is liable for the actions of its staff and Governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether personal data handling is sensitive or routine.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the GDPR) and the Data Protection Act 2018 (DPA 2018). The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (**ICO**) is responsible for enforcing data protection law, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

1. Definitions

Key data protection terms covered by this data protection policy are defined as:

- **Data controller** – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including its Governors) is the controller. An independent contractor who makes its own such decisions is also, separately, likely to be a data controller.

- **Data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.

- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- **Personal Data -** any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.

- **Processing** – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.

- **Special categories of personal data –** data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

- **Automated Decision-Making (ADM**) – the process of making decisions using automation without direct human involvement, such as an online decision to award financial support, an online admissions test or a recruitment aptitude test, which uses pre-programmed algorithms and criteria.

- **Automated Processing** – where a human inputs the data to be processed, and then the decision-making is carried out by an automated system, such as may be used by a profiling system.

- **Consent** - any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

- **Data Breach** - is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- **Data Protection by Design** – the process of designing data protection by referencing Data Protection Impact Assessment requirements in all risk, project and change management procedures.

- **Data Protection Impact Assessment (DPIA)** - the process of systematic analysis which helps to identify and minimise the data protection risks of a project or plan.

- **Data Protection Officer (DPO)** - UK GDPR encompasses a duty to appoint a data protection officer (DPO) if an organisation is a public authority or a body that carries out certain types of processing activities. This applies to core activities requiring large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking), or processing on a large scale of special category data, or data relating to criminal convictions and offences.

- **Data subject** - the identified or identifiable living individual to whom personal data relates.

- **Legitimate Interest Assessment** – the process which identifies whether data can be processed on the basis of a legitimate interest, the benefits of the processing and whether it is necessary.

- **Privacy Notice** – the document which sets out for people what is being done with personal data. Individuals have the right to know why data is needed, what will be done with it and with whom it will be shared. In particular, this information should be provided in a clear, open and honest way.

- **Related Policies** – there are a number of other policies at the school, which are related to the Data Protection Policy as follows:

  a) Acceptable Use policy
  b) e-Safety policy
  c) Safeguarding policy
  d) Social media policy
  e) Photographic images policy
  f) Admissions Policy
  g) Recruitment, Selection and Retention Policy
  h) Secondary/Destination School Policy

2. Application of this policy

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

Those who handle personal data as employees or Governors of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as "data processors" on the School's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party data controllers – which may range from other schools, to parents, to appropriate authorities, to casual workers and volunteers – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy. Where required, the school will ensure that suitable data sharing agreements are in place and that staff, parents and Governors are advised of the data sharing as necessary.

If you are a contractor, you will be a data controller in your own right, but the same legal regime and best practice standards set out in this policy will apply to you by law.

3. Person responsible for Data Protection at the School

The School has appointed the Head as the Data Protection Lead, as the School is not required to appoint a Data Protection Officer within the meaning of GDPR. The Lead is supported by a Data Protection Team (DPT) comprising the Bursar and Network Manager. The School through the DPT will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of applicable data protection legislation. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Lead.

4. The Principles

The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **Relevant** and **limited** to what is necessary for the purposes it is processed;
4. **Accurate** and kept **up to date**;
5. **Kept for no longer than is necessary** for the purposes for which it is processed; and
6. Processed in a manner that ensures **appropriate security** of the personal data.

The GDPR's broader 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments when required); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

5. Lawful grounds for data processing

Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the School. Legitimate interest assessments (LIA) are undertaken whenever a data audit takes place and data processing activities arise. These activities may also be undertaken in direct response to changes in legislation, or during the regular review cycles of this policy.

Legitimate interest can be challenged by data subjects and means the School is taking on extra responsibility for considering and protecting people's rights and interests. The outcome of any LIA is included in the School's identified legitimate interests, which are set out in its Privacy Notice, as required by the UK GDPR.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds, as set out in the Privacy Notice.

6. Headline responsibilities of all staff

Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that *any* personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to **record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it**.

Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with the staff handbook and all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, and all staff should read and comply with the policies listed in Section 2 above.

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

Avoiding, mitigating and reporting data breaches

One of the key obligations contained in the GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If staff become aware of a personal data breach they must notify the DPT. If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs to know about them to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

Care and data security

More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see Section 3 above), and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School. Appropriate training will be provided for management staff in order to support them with this responsibility and to assist them with identifying the need for regular staff training, whether this be delivered by management or by other specialist training providers. Staff must attend any training the school requires them to.

7. Rights of Individuals

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Parents may also make educational record requests, which are not treated in the same way as full subject access requests.

Such requests, either subject access or educational record requests, must be dealt with promptly in line with the school's documented process for dealing with the same. A record of data subject access requests will also be maintained. If someone becomes aware of a subject access request (or indeed any communication from an individual about their personal data), the Head must be informed as soon as possible. Data subject rights are dealt with as quickly as possible and within the periods specified by legislation. However, individuals making such requests need to be aware that dealing with the requests fully and appropriately will take the time the process needs, especially where the engagement of additional resources or professional services is required. In such an event, data subjects would be informed should any circumstances arise which would cause reasonably unavoidable delays to the process.

Individuals also have legal rights to:

- require the school to correct the personal data held about them if it is inaccurate;
- request that the school erase their personal data (in certain circumstances);
- request that the school restrict its data processing activities (in certain circumstances);
- receive from the school the personal data held about them for the purpose of transmitting it in a commonly used format to another data controller; and
- object, on grounds relating to their particular situation, to any of the school's particular processing activities where the individual feels this has a disproportionate impact on them.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- object to direct marketing; and
- withdraw one's consent where the school is relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, if a request is received from an individual who is purporting to exercise one or more of their data protection rights, the Head must be informed as soon as possible.

8. Data Security: online and digital

The School has an absolute duty to ensure that personal data is kept secure by appropriate technical and organisational measures in order to ensure a level of security appropriate to the risk. This means that the School must ensure that appropriate security measures are in place to prevent unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Unless there is no reasonable alternative, personal data does not leave the school's secure systems. In the unlikely event that this become necessary:

- No member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Head or Bursar.
- No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.
- Where a worker is permitted to take data offsite on memory sticks or personal devices it must be encrypted.
- Use of personal email accounts or unencrypted personal devices by Governors or staff for official School business is not permitted.

9. Summary Policy Statement

It is the intention of this policy that the following requirements and considerations are met by way of the data management processes and reviews:

- Complying with the Accountability Principle requirements;
- Consent;
- Transparency – notifying/communicating with data subjects and parents;
- Purpose limitation in data processing;
- Data minimisation;
- Accuracy of data;
- Storage limitation and data destruction;
- The confidentiality, integrity and availability of data;
- Data protection and safeguards;
- Data transfers;
- Managing data subject rights;
- Meeting the Accountability Principle requirements;
- Record keeping;
- Training (for management and staff);
- Monitoring, review and audit;
- Implementing Data Protection by Design and by Default;
- Data Protection Impact and risk assessments;
- Data mapping and the Record of Processing Activities;
- Automated Processing (including profiling) and Automated Decision-Making;
- Use of data for marketing purposes; and
- Data Protection Policy monitoring, review and changes.

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which staff and Governors come into contact, fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?

- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?

- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.

Stormont School

ANNEX A

PRIVACY NOTICE

Applicable to staff, parents and pupils (past and present)

WHO WE ARE

Stormont School ("the School") is a company limited by guarantee, registration number 726450 and a charity with a registration number of 311079. For day to day communications, the School is referred to as Stormont. For the purposes of this Privacy Notice, the School does not include the Stormont Old Girls' Association or the Stormont Parents' Association both of which have separate charitable status. The School is established to promote and provide for the provision of education of girls in the United Kingdom, which it does by operating the School as an independent day School for girls aged from 4 to 11 years. The School is a Data Controller for the purposes of Data Protection Law which means it determines how an individual's personal data is processed and for what purposes.

WHAT THIS PRIVACY NOTICE IS FOR

This notice is intended to provide information about how the School will use (or "process") personal data about individuals including: its current, past and prospective pupils; and their parents, carers or guardians (referred to in this notice as "parents").

In accordance with the Data Protection Act 1998 ('the Act'), the School is registered with the Information Commissioner's Office (ICO) regarding its processing activities. The School's ICO registration number is Z5413614 and its registered address is Stormont School, The Causeway, Potters Bar, EN6 5HA.

This information is provided in accordance with Data Protection Law which gives individuals rights to understand how their data is used. Staff and parents ~~and pupils~~ are all encouraged to read this Privacy Notice and understand the School's obligations to its entire community.

This **Privacy Notice** applies alongside any other information the School may provide about a particular use of personal data, for example when collecting data via an online or paper form.

This **Privacy Notice also** applies in addition to the School's other relevant terms and conditions and policies, including:

- any contract between the School and its staff or the parents of pupils;
- the School's policy on taking, storing and using images of children;
- the School's retention of records policy;
- the School's safeguarding, pastoral, or health and safety policies, including as to how concerns or incidents are recorded; and
- the School's IT policies, including its Acceptable Use and eSafety policy.

Anyone who works for, or acts on behalf of, the School (including staff, volunteers, governors and service providers) should also be aware of and comply with ~~this Privacy Notice~~ the school's Data Protection Policy.

RESPONSIBILITY FOR DATA PROTECTION

The School has set up a Data Protection Team led by the Head, which will deal with your requests and enquires concerning the School's use of your personal data (see section on 'Your rights' below) and endeavour to ensure that all personal data is processed in compliance with this policy and Data Protection Law. Requests and enquiries should be sent to data@stormontschool.org or in writing to Stormont School, The Causeway, Potters Bar, EN6 5HA.

WHY THE SCHOOL NEEDS TO PROCESS PERSONAL DATA

In order to carry out its ordinary duties to staff, pupils and parents, the School needs to process a wide range of personal data about individuals (including current, past and prospective staff, pupils or parents) as part of its daily operation.

Some of this activity the School will need to carry out in order to fulfil its legal rights, duties or obligations – including those under a contract with its staff, or ~~the~~ parents of its pupils.

Other uses of personal data will be made in accordance with the School's legitimate interests, or the legitimate interests of another, provided that these are not outweighed by the impact on individuals, and provided it does not involve special or sensitive types of data.

The School expects that the following uses will fall within that category of its (or its community's) "**legitimate interests**":

- To safeguard pupils' welfare and provide appropriate pastoral care;
- To fulfil our contractual and legal obligations;
- For the purposes of pupil admission (and to confirm the identity of prospective pupils and their parents);
- To provide education services, including musical education, physical training or spiritual development and extra-curricular activities to pupils, and monitoring pupils' progress and educational needs;
- Maintaining relationships with alumni and the School community, including direct marketing or fundraising activity;
- For the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law (such as tax or diversity analysis);
- To enable relevant authorities to monitor the School's performance and to intervene or assist with incidents as appropriate;
- To give and receive information and reports about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils;
- To enable pupils to take part in national or other assessments including those associated with application to secondary or other destination schools, and to publish achievements of pupils of the School;
- To monitor (as appropriate) use of the School's IT and communications systems in accordance with the School's Acceptable Use Policy;
- To make use of photographic images of pupils in School publications, on the School website and (where appropriate) on the School's social media channels in accordance with the School's policy on taking, storing and using images of children;
- To carry out or cooperate with any internal School or external complaints, disciplinary or investigation processes; and
- Where otherwise reasonably necessary for the School's purposes, to obtain appropriate professional advice and insurance for the School.

In addition, the School will on occasion need to process **special category personal data** (concerning health, ethnicity, and religion) or criminal records information (such as when carrying out DBS checks) in accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required. These reasons will include:

- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's medical condition or other relevant information where it is in the individual's interests to do so: for example for medical advice, for child protection, safeguarding, and cooperation with police or social services, for insurance purposes or to caterers or organisers of School trips who need to be made aware of dietary or medical needs;
- For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with its legal obligations and duties of care;
- As part of any School or external complaints, disciplinary or investigation process that involves such data, for example if there are SEN, health or safeguarding elements;
- To provide educational services in the context of any special educational needs of a pupil;
- To provide spiritual education in the context of any religious beliefs;
- In connection with the recruitment ~~of volunteers~~ and employment of its staff, for example DBS checks, welfare, or pension plans.

TYPES OF PERSONAL DATA PROCESSED BY THE SCHOOL

This will include by way of example:

- names, addresses, telephone numbers, e-mail addresses and other contact details;
- bank details and other financial information, e.g. about parents who pay fees to the School;
- past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs);
- past, present and prospective parents' employment information;
- records of parents who act as volunteers;
- personnel files, including in connection with academics, employment or safeguarding;
- where appropriate, information about individuals' health and welfare, and contact details for their next of kin;
- references given or received by the School about pupils, and relevant information provided by previous educational establishments and/or other professionals or organisations working with pupils;
- correspondence with and concerning pupils and parents past and present; and
- images of pupils (and occasionally other individuals) engaging in School activities, (in accordance with the School's policy on taking, storing and using images of children)
- car details for those using parking on site.

HOW THE SCHOOL COLLECTS DATA

Generally, the School receives personal data from the ~~parents~~ individual directly (including, in the case of pupils, from their parents). This may be via a form, or simply in the ordinary course of interaction or communication (such as email or written assessments).

However, in some cases personal data will be supplied by third parties with the consent of the parents (for example another School, or other professionals or authorities working with that individual). It may also be collected from publicly available sources.

WHO HAS ACCESS TO PERSONAL DATA AND WHO THE SCHOOL SHARES IT WITH

Occasionally, the School will need to share personal information relating to its community with third parties, such as:

- professional advisers (e.g. lawyers, insurers, PR advisers, Bursary and Finance agencies and accountants);
- educational providers (e.g. educational advisers);
- government authorities (e.g. HMRC, DfE, the police or the local authority);
- appropriate regulatory bodies (e.g. the **Independent Schools Inspectorate**, the Charity Commission or the Information Commissioner).

For the most part, personal data collected by the School will remain within the School, and will be processed by appropriate individuals only in accordance with access protocols (i.e. on a 'need to know' basis). Particularly strict rules of access apply in the context of:

- medical records held by the School and accessed only by appropriate staff under the authorisation of the safeguarding lead, or otherwise in accordance with express consent;
- pastoral or safeguarding files.

However, a certain amount of any medical, pastoral and SEN pupil's relevant information will need to be provided to staff more widely in the context of providing the necessary care and education that each pupil requires.

Staff, pupils and parents are reminded that the School is under duties imposed by law and statutory guidance (including Keeping Children Safe in Education) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This is likely to include file notes on safeguarding files, and in some cases referrals to relevant authorities such as the LADO or the police. For further information about this, please view the School's Safeguarding ~~(Child protection)~~ Policy.

For the purposes of maintaining a safe and secure environment, the School reserves the right to monitor all internet traffic through its filtering systems and all domain-joined devices through e-Safe monitoring software and services.

Finally, in accordance with Data Protection Law, some of the School's processing activity is carried out on its behalf by third parties, such as IT systems, web developers or cloud storage providers. This is always subject to contractual assurances that personal data will be kept securely and only in accordance with the School's specific directions.

HOW LONG WE KEEP PERSONAL DATA

The School will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Typically, the legal recommendation for how long to keep ordinary pupil files is up to the child's 25th birthday and for ordinary staff personnel files, it is up to 7 years following departure from the school. However, incident reports and safeguarding files will need to be kept much longer, in accordance with specific legal requirements.

If you have any specific queries about how our retention policy is applied, or wish to request that personal data that you no longer believe to be relevant is considered for erasure, please contact the Data Protection Team (data@stormontschool.org). However, please bear in mind that the School will often have lawful and necessary reasons to hold on to some personal data **even following such a request.**

A limited and reasonable amount of information will be kept (for archiving purposes) for example. Even where you have requested we no longer keep in touch with you, we will need to keep a record of this fact in order to fulfil your wishes (called a "suppression record").

KEEPING IN TOUCH AND SUPPORTING THE SCHOOL

The School will use the contact details of parents, alumni and other members of the School community to keep them updated about the activities of the School, including by sending updates and newsletters, by email and by post. Unless the relevant individual objects, the School will also:

- Share personal data about parents and/or alumni, as appropriate, with organisations set up to help establish and maintain relationships with the School community, such as The Stormonts' Parents' Association and The Stormont Old Girls (alumni);
- Contact parents and/or alumni (including via the organisations above) by post and email in order to promote and raise funds for the School and, where appropriate, other worthy causes;

Should you wish to limit or object to any such use, or would like further information about them, please contact the Data Protection Team in writing. You always have the right to withdraw consent, where given, or otherwise object to direct marketing or fundraising.

However, the School is nonetheless likely to retain some of your details (not least to ensure that no more communications are sent to that particular address, email or telephone number).

YOUR RIGHTS

- Rights of access.

Individuals have various rights under Data Protection Law to access and understand personal data about them held by the School, and in some cases ask for it to be erased or amended or have it transferred to others, or for the School to stop processing it, subject to certain exemptions and limitations.

Any individual wishing to access or amend their personal data, or wishing it to be transferred to another person or organisation, or who has some other objection to how their personal data is used, should put their request in writing to the Data Protection Team.

The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time limits (which is one month in the case of requests for access to information).

The School will be better able to respond quickly to smaller, targeted requests for information. If the request for information is manifestly excessive or similar to previous requests, the School may ask you to reconsider, or require a proportionate fee (but only where Data Protection Law allows it).

- Requests that cannot be fulfilled.

You should be aware that the right of access is limited to your own personal data, and certain data is exempt from the right of access. This will include information which identifies other individuals (and parents need to be aware this may include their own children, in certain limited situations – please see further below), or information which is subject to legal privilege (for example legal advice given to or sought by the School, or documents prepared in connection with a legal action).

The School is also not required to disclose any pupil examination scripts (or other information consisting solely of pupil test answers), provide examination or other test marks ahead of any ordinary publication, nor share any confidential reference given by the School itself for the purposes of the education, training or employment of any individual.

You may have heard of the "right to be forgotten". However, we will sometimes have compelling reasons to refuse specific requests to amend, delete or stop processing your (or your child's) personal data: for example, a legal requirement, or where it falls within a legitimate interest identified in this Privacy Notice. All such requests will be considered on their own merits.

- Pupil requests.

Pupils where supported by parents can make subject access requests for their own personal data. Pupils at Stormont are not generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested, including any relevant circumstances at home. A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf although this will depend on both the child and the personal data requested, including any relevant circumstances at home.

While a person with parental responsibility will generally be entitled to make a subject access request on behalf of younger pupils, the law still considers the information in question to be the child's.

- Parental requests.

It should be clearly understood that the rules on subject access are not the sole basis on which information requests are handled. Parents may not have a statutory right to information, but they and others will often have a legitimate interest or expectation in receiving certain information about pupils without their consent. The School may consider there are lawful grounds for sharing with or without reference to that pupil.

Parents will in general receive educational and pastoral updates about their children. Where parents are separated, the School will generally aim to provide the same information to each person with parental responsibility, but may need to factor in all the circumstances including the express wishes of the child.

All information requests from, on behalf of, or concerning pupils – whether made under subject access or simply as an incidental request – will therefore be considered on a case by case basis.

- Consent.

Where the School is relying on consent as a means to process personal data, any person may withdraw this consent at any time (subject to similar age considerations as above). Please be aware however that the School may not be relying on consent but have another lawful reason to process the personal data in question even without your consent.

That reason will usually have been asserted under this Privacy Notice, or may otherwise exist under some form of contract or agreement with the individual (e.g. an employment or ~~a~~ parent contract, or because a purchase of goods or services, or membership of an organisation such as an alumni or parents' association has been requested).

- Whose rights?

The rights under Data Protection Law belong to the individual to whom the data relates. However, the School will often rely on parental consent to process personal data relating to pupils (if consent is required) unless, given the nature of the processing in question and the pupil's age and understanding, it is more appropriate to rely on the pupil's consent. Parents should be aware that in such situations they may not be consulted, depending on the interests of the child and the parents' rights at law or under their contract.

In general, the School will assume that pupils' consent is not required for ordinary disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the

pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the School's opinion, there is a good reason to do otherwise.

However, 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, the School may be under an obligation to maintain confidentiality unless, in the School's opinion, there is a good reason to do otherwise; for example, where the School believes disclosure will be in the best interests of the pupil or other pupils, or if required by law.

Pupils are required to respect the personal data and privacy of others, and to comply with the School's relevant policies, e.g. ~~IT:~~ Acceptable Use Policy and the School rules. Staff are under professional duties to do the same, covered under the Data Protection Policy and other relevant staff policies.

DATA ACCURACY AND SECURITY

The School will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must notify the School of any significant changes to important information, such as contact details, held about them. The responsibility for changes in information relating to pupils, rests with the parent.

An individual has the right to request that any out-of-date, irrelevant or inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under Data Protection Law). Please see above for details of why the School may need to process your data, and whom you may contact if you disagree.

The School will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to School systems. All staff and governors will be made aware of this policy and their duties under Data Protection Law and will receive relevant training.

THIS NOTICE

The School will update this Privacy Notice from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.

QUERIES AND COMPLAINTS

Any comments or queries on this notice should be directed to the Head or the Bursar using the following contact details: admin@stormontschool.org.

If an individual believes that the School has not complied with this notice or acted otherwise than in accordance with Data Protection Law, they should follow the School complaints procedure. You can also make a referral to, or lodge a complaint with, the Information Commissioner's Office (ICO), although the ICO recommends that steps are taken to resolve the matter with the School before involving the regulator.

Reviewed 28th April 2021