KILGRASTON SCHOOL

DATA PROTECTION POLICY (GDPR)

1. Introduction

Kilgraston School ("the School") must process personal data in compliance with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (the "DPA").

The purpose of this policy is to give staff some basic information about the main rights within and the requirements of the DPA. It is also to direct them to seek further guidance where necessary.

It is important that staff read this document carefully and understand their responsibilities under the DPA as any breach of this policy will be taken seriously and may result in disciplinary action. You should also be aware that the DPA imposes individual responsibility and failure to comply may result in you being personally liable for a criminal offence. This Policy should be read in conjunction with the School's Privacy Statement

The Data Protection Act 2018 sets out the frame work for data protection law in the UK. It sets out key principles, rights and obligations for most processing of personal data.

2. Definitions

Personal data – data consisting of information relating to a living individual who can be identified from that information (or from that and other information likely to come into the possession of a data controller), including any expression of opinion about the individual or indication of the intentions of the data controller or any other person in respect of that individual. In practice, this means any information from which a living individual can be identified either directly or indirectly.
Special Category data (also known as sensitive personal data) are certain types of personal data that are afforded extra protection under the DPA. That is personal data about a person's racial or ethnic origin, political opinions, religious or other similar beliefs, trade union membership, physical or mental health or condition, sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal or sentence of any court in such proceedings.

Data Controllers – those who hold and process data

Data Processors – those who process data on behalf of a Data Controller

Data Subject – those who have their data held. The school is a registered data controller and its registration can be viewed online at: https://ico.org.uk/ESDWebPages/Entry/Z6186366

Data Protection Officer – the individual with responsibility for data protection in the School. For Kilgraston, this is the Head of Finance.

Processing – is any activity that involves obtaining, recording or holding the data, or carrying out any operation or set of operations on data including organising, amending, retrieving, using, disclosing, erasing or destroying it.

3. The Principles

When processing personal data the School must comply with the 8 data protection principles which underpin the DPA.

1). Personal data shall be processed fairly and lawfully and in particular, shall not be processed unless at least one of the conditions in Schedule 2 of the DPA is met, and in the case of sensitive personal data, at least one of the conditions in Schedule 3 of the DPA is also met .

2). Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3). Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4). Personal data shall be accurate and, where necessary, kept up to date.

5). Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6). Personal data shall be processed in accordance with the rights of data subjects under the DPA.

7). Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8). Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Duties of Employees

Employees of the School should:

- Read and understand this document;
- Familiarise themselves with and abide by the Data Protection principles;
- Understand how to meet the expected standards at any stage in the life-cycle of data;
- Understand how to safeguard the rights of data subjects;
- Understand what is meant by ‘personal data’ and ‘sensitive personal data’;
- Seek guidance from a member of the senior management team if unsure at any stage;
- Ensure their own personal data held by the School is accurate and up to date;
- Securely store personal data, whether in physical or electronic files.
- Only use the School emails accounts and systems for work purposes.
- Only use USB or other removable devices if they are encrypted.

- Pass any requests relating to personal data (from the individual or a third party) to the Data Protection Officer.

Employees of the School should not:

- Leave personal data unattended or in such circumstances where third parties may gain access to them.
- Disclose any information about pupils, parents, staff or other data subjects unless they are clear they have permission to do so;
- Provide references without first obtaining the consent of the individual involved and authorisation of SMT;
- Disclose personal data to the police or any other public authority or third party without first obtaining the consent of Data Protection Officer or in their absence a member of SMT.

5. Lifecycle of Data

One way of looking at the data held by the School is in terms of the lifecycle of data:

- Creation/acquisition;
- Holding;
- Processing;
- Querying;
- Amending;
- Editing;
- Disclosure or transfer to third parties;

And

- Destruction.

6. Best Practice Guidelines for the lifecycle

To comply with the data protection principles of the DPA, records containing personal data must be:

- Stored appropriately (securely with regulated access)
- Retained for only as long as necessary
- Disposed of securely

Creation/acquisition – in most cases, anyone wishing to gather/ process personal data must tell the data subjects the purpose for which they are gathering the data; in other words, they must have a lawful basis for processing the data; there are a number of different 'lawful bases' for processing personal data including consent, contract, legal obligation and legitimate interest. Where the data being processed is sensitive personal data, further lawful bases is required, for example explicit consent.

Holding - personal data should not be held for longer than necessary (see recommended retention periods in the School's retention policy) and should be checked regularly to ensure it is still accurate, up to date and still needs to be retained. Measures should be taken to safeguard data to prevent loss, destruction or unauthorised disclosure. As a general rule, the more sensitive the data is, the more measures that should be put in place to protect it.

Processing, querying, editing, amending, - only process personal data that is required for a specified purpose, otherwise the consent of the data subject should be informed and where necessary their consent sought.

Disclosures – the School wishes to protect the confidentiality of data it holds therefore employees must abide by the rules set out in 'Duties of Employees'.

Transfers – there should be no need to transfer personal data to another country or outside the EEA however if such a need arises then permission should be sought from the Data Protection Officer.

Destruction – data should not be held for longer than necessary and then shredded securely to prevent possible misuse or in the case of electronic files deleted by the appropriate person.

7. Processing in line with individual's rights

Personal data must be processed in line with the rights of individuals. Individuals have the right to:

- Request access to any of their personal data held by a data controller (subject access request)
- Prevent the processing of their personal data for direct marketing purposes
- Have inaccurate personal data corrected/ erased
- Prevent processing that is likely to cause substantial and unwarranted damage and distress (section 10 notice)

Subject Access Rights

Individuals have the right to access to personal data about themselves held by the School, subject to certain exemptions and limitations set out in the DPA. A subject access request is a request for information about the requester, it does not need to mention that it is a subject access request or cite the DPA.

Any data subject wishing access to their personal data will be required to make such a request in writing to the School. The school may charge a reasonable fee for the administrative cost of complying with the request and if necessary ask for proof of identity, a mandate or further information reasonably required to allow the personal data to be located. Any such request must be passed to the Data Protection Officer as soon as possible. The School will normally respond to the request within 30 calendar days and in accordance with the School's Guidance on Information Requests.

Please note that under **The Pupils' Educational Records (Scotland) Regulations 2003**, parents/ guardians of pupils have a separate right of access to their child's Education Record. Any such request should also be forwarded to the Data Protection Officer who will respond in accordance with the legislation/ the School's Guidance on Information Requests. The timescale for responding is 15 school days.

Right to Prevent Processing of Personal data ("section 10 notice")

Under DPA individuals have the right to request that a data controller cease, or not begin processing, their personal data where it causes them unwarranted substantial damage or distress. If you receive a request from an individual requesting that the School stop processing (or do not start processing) their personal data, this must be passed to the Data Protection Officer as soon as possible. If is for

the Data Protection Officer to determine how to respond to the notice and issue that response without undue delay.

Requests to correct inaccurate data

An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the DPA). Any such request should be directed to the Data Protection Officer.

Third party requests for personal data

Staff should not disclose personal data, including of students, parents, staff, governors, unless they are clear they have permission to do so. Therefore, if you receive a request from a third party for personal data, such as a request from another School, official agency, the Police or even a relative it should be forwarded to the Data Protection Officer, or in their absence (and if the matter is urgent) a member of the School's Senior Management Team.

8. Data Accuracy

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 and will conduct regular reviews. However, all staff who provide personal data to the School are responsible for ensuring that the personal data they provide to the School is accurate at the time it is given, and for informing the School of any changes to the personal data that they have provided to it, e.g. change of address. The School cannot be held responsible for any errors in the personal data it holds unless the staff member informs them of such changes. Individuals must notify the Data Protection Officer of any changes to personal data they have provided.

9. Data Security

The School will take appropriate technical and organisational steps to ensure the security of personal data about individuals. All staff will be made aware of this policy and their duties under the DPA, including through regular training.

Security procedures are set out in the School's Information Security Policy and Information Technology Staff Use Policy and include:

- Reporting any unaccompanied stranger in the School.
- Locking desks, cupboards and filing cabinets with personal data.
- Not leaving personal data unattended where third parties may gain access.
- Securely shredding paper documents and passing USB sticks, CDs and other electronic equipment that is no longer required to ICT to arrange for the data to be securely destroyed/ disposed of.
- Ensuring that if staff are looking at sensitive personal data monitors are positioned in such a way that they can't be seen by passers-by and that PCs are locked when left unattended.
- All devices used for School work, such as laptops, tablets or phones should be approved by ICT to ensure that appropriate security measures are in place.
- Encrypting and password protecting removable equipment such as USB sticks and CDs that contain personal data.

- Ensuring passwords are complex and kept confidential. The School will require passwords to be changed regularly.
- Only using School email accounts and systems for work purposes, staff should not send personal data to their personal email accounts or save personal data to their own devices.
- Staff should only access personal data required for their role and the School has measures in place to restrict access to sensitive personal data.

10. Homeworking, Devices and taking personal data outside the School

As above, only your School email account should be used for work purposes. If you require remote access to your School email account or the School systems then this should be authorised by your line manager and the Data Protection Officer. In assessing and deciding whether it is appropriate for you to access your School email account (and where necessary the School systems) remotely and on your own device, the School will have regard to the ICO's guidance on Bring Your Own Device and the School's obligations under the DPA. Where you will be using your own device (computer, tablet, phone), the ICT department will ensure you have secure access to your School email / systems as required.

Personal data should only be removed from the School where necessary e.g. to attend a meeting or go on an excursion/ school trip. In particular, sensitive personal data should never be removed from the School unless this is absolutely necessary. When outside the School papers should not be left unattended and must be kept within your sight at all times. Laptops, USBs, CDs etc. should be encrypted and password protected.

When you cease your employment with the School any equipment belonging to the School must be safely returned and the School will revoke any remote access granted.

11. Retention Periods for Data Protection Purposes

The DPA does not set out minimum or maximum retention periods. However, the emphasis under GDPR and the DPA is that personal data and sensitive personal data should not be kept longer than is necessary for the purposes for which it is processed. This means that the School will securely destroy or delete personal data from our systems when it is no longer required. How long the School is required to keep personal data will depend on the nature of the personal data, the purposes for which it is processed and any other legal requirements the School is under to retain in. How long information is held for should be decided on a case by case basis but the School has developed a Retention Policy which sets out, in general, how long different types of personal data will be kept.

In assessing how long to keep personal data, the School will consider:

- what the information was gathered for and is used for;
- the current and future value of the information;
- any statutory requirement to retain the information;
- any professional/ sector guidance on retaining the information;
- the costs, risks and liabilities associated with retaining or not retaining the information; and
- the ease or difficulty of making sure it remains accurate and up to date.

There are certain legal or regulatory requirements in terms of the retention of data such as information needed for tax, health and safety or audit purposes. Staff responsible for records management should check from time to time to ensure practice remains in line with requirements.

12. What to do in the event of a DPA security breach?

Any breach (actual, alleged or suspected) of DPA security should be reported as soon as possible to the Data Protection Officer and in their absence another member of the SLT. A breach includes unauthorised access to, accidental loss of, damage or destruction to personal data. The school must report a notifiable breach to the ICO without undue delay and not later than 72 hours after becoming aware of it. Where it takes longer than this to report a breach, the school must be prepared to provide reasons for the delay.

13. Compliance

As mentioned at the start of the policy, failure to comply with this policy could result in disciplinary action being taken against you under the School Disciplinary Policy. It may also be a criminal offence to misuse or disclose personal data without authorisation. Staff should ensure they are familiar with their responsibilities under the DPA and seek guidance if they are ever unsure. Should staff have any questions or concerns in relation to the processing of personal data these should be directed to the Data Protection Officer, and in their absence another member of SLT.

Policy Review Record

Person responsible – Head of Finance

Date	Action	Reason	Review complete	Initials
July 2017	Annual Review		31/7/2017	BF
September 2017	Staff training	Briefing		BF
September 2018	Annual Review		10/9/2018	BF
July 2020	Annual Review		29/7/2020	Square Peg HR
September 2020	Annual Review		4/9/2020	MM