Marjory Kinnon School

Data Protection Policy

October 2019

Approved by the Resources Committee: October 2019

Our school collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations. Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Privacy Notice to all staff and volunteers; this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

1. Purpose

This Policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 2018, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

2. What is Personal Information

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

3. Data Protection Principles

The Data Protection Act 2018 establishes eight enforceable principles that must be adhered to at all times:

- Personal data shall be processed fairly and lawfully.
- Personal data shall be obtained only for one or more specified and lawful purposes.
- Personal data shall be adequate, relevant and not excessive.
- Personal data shall be accurate and where necessary, kept up to date.
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 2018.
- Personal data shall be kept secure i.e. protected by an appropriate degree of security.

- 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 data protection.

4. General Statement

The school is committed to maintaining the above principles at all times. Therefore, the school will:

- Inform individuals why the information is being collected when it is collected.
- Inform individuals when their information is shared, and why and with whom it was shared.
- Check the quality and the accuracy of the information it holds.
- Ensure that information is not retained for longer than is necessary.
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely.
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Share information with others only when it is legally appropriate to do so.
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests (SAR).
- Ensure our staff are aware of and understand our policies and procedures.

5. Procedures for Responding to Subject Access Requests made under the Data Protection Act 2018

5.1 Rights of Access to Information

There are two distinct rights of access to information held by schools about pupils.

1. Under the Data Protection Act 2018 any individual has the right to make a request to access the personal information held about them.
2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004. These procedures relate to subject access requests made under the Data Protection Act 2018.

5.2 Actioning Subject Access Requests

1. Requests for information must be made in writing; which includes email, and be addressed to the Headteacher. If the initial request does not clearly identify the information required, then further enquiries will be made.
2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- Passport.
- Driving licence.
- Utility bills with the current address.
- Birth / Marriage certificate.
- P45/P60.
- Credit Card or Mortgage statement.

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However, with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school may make a charge for the provision of information, dependent upon the following:

- Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
- Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.
- If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the School.

5. The response time for subject access requests, once officially received, is 40 days (not working or school days but calendar days, irrespective of school holiday periods). However, the 40 days will not commence until after receipt of fees or clarification of information sought.
6. The Data Protection Act 2018 allows exemptions as to the provision of some information; therefore, all information will be reviewed prior to disclosure.
7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40-day statutory timescale.
8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.
9. If there are concerns over the disclosure of information, then additional advice should be sought.
10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.
11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.
12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face-to-face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used.

6. Data Breaches

On finding or causing a breach, or potential breach, the staff member or Data Controller (Mark O'Brien, Chief Operating Officer) must immediately notify the Data Protection Officer (DPO). The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost.
- Stolen.
- Destroyed.

- Altered.
- Disclosed or made available where it should not have been.
- Made available to unauthorised people.

The DPO will alert the Headteacher and the Chief Operating Officer. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or Data Controller (Mark O'Brien, Chief Operating Officer) where necessary. (Actions relevant to specific data types are set out at the end of this procedure).

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data.
- Discrimination.
- Identify theft or fraud.
- Financial loss.
- Unauthorised reversal of pseudonymisation (for example, key-coding).
- Damage to reputation.
- Loss of confidentiality.
- Any other significant economic or social disadvantage to the individual(s) concerned.
- If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's online compliance system (EVERY).

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned.
  - The categories and approximate number of personal data records concerned.
- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the Police, insurers, banks or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause.
- Effects.
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

Records of all breaches will be stored on the EVERY system.

The DPO, Headteacher and/or Chief Operating Officer will review what happened and how it can be stopped from happening again. This will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

The school will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. The school will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)	• If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error. • Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error. • If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT Team to recall it. • In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way. • The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

	• The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
Details of pupil premium interventions for named children being published on the school website	• Only previously authorised and trained members of staff have authority to upload information to the public website.
Non-anonymised pupil exam results or staff pay information being shared with governors	• The process for the Teachers Pay Panel stipulates only anonymised data is provided to Governors on the Pay Panel and in the report back to the Full Governing Body (FGB). • All pupil data shared with the Governing Body is anonymised.
A school laptop containing non-encrypted sensitive personal data being stolen or hacked	• Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, management information systems (MIS) and/or learning platform. • Staff adhere to e-Safety Policy guidance (Appendix B – School Devices Used Off-Site) which stipulates the use of approved and secure email systems and managed learning environment (MLE) tools and that personal data is only taken out of school or accessed remotely with the prior authorisation of the Headteacher or Governing Body. • Staff laptops used at home are protected by Sophos Anti-Virus.

The school's cashless payment provider being hacked and parents' financial details stolen	• The school expects any prospective provider to provide appropriate guarantees in respect to putting technical and organisational measures in place to protect personal data and the rights of data subjects. When introducing new systems, the school will undertake an impact assessment with advice and assistance from the DPO.

7. Complaints

Complaints about the above procedures should be made to the Chair of Governors who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's Complaints Procedure. Complaints which are not appropriate to be dealt with through the school's Complaints Procedure may be referred to the Information Commissioner (the statutory regulator). Contact details of both will be provided with the disclosure information.

8. Contacts

If you have any enquires in relation to this Policy, please contact Mark O'Brien, Chief Operating Officer (COO) who is appointed as the school's Data Controller. The school's Data Protection Officer is:

Judicium Consulting Limited

Address: 72 Cannon Street, London, EC4N 6AE

Email: dataservices@judicium.com

Telephone: 020 3326 9174

Web: www.judiciumeducation.co.uk

Lead Contact: Craig Stilwell

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 5457453.

9. Review

This Policy will be reviewed as it is deemed appropriate, but no less frequently than the statutory guidance of at least every 2 years. The Policy review/approval (determined by the Governing Body) is assigned to the Resources Committee.

10. Acronyms

COO	Chief Operating Officer
DPO	Data Protection Officer
EVERY	The school's online compliance system
ICO	Information Commissioner's Office
ICT	Information and communications technology
MIS	Management information systems
MLE	Managed learning environment
SAR	Subject Access Requests

Appendix A

10 Steps to take for GDPR Compliance

1	**Secure Your Machine**	• Access to desktop/laptop is password protected. • Change passwords regularly. • Lock machines (ctrl+alt+del to lock computer).
2	**Don't Give Out Sensitive Information**	• Don't give out confidential information over the phone. • Send information securely/encrypted if needed. • Store passwords safely – not on post-it notes.
3	**Secure Your Documents**	• Encrypt/password protect documents where possible. • Limit access to shared drives which contain confidential information.
4	**Paper Documents**	• Clean desk policy? • Keep sensitive paper documents off your desk. • Shred and file papers as matter of course. • Lock sensitive documents in draw/filing cabinet. • Who has access to keys? Don't leave them in the door.
5	**Be Careful With Remote Access & Storage Devices**	• Accessing confidential documents remotely – ensure adequate security (e.g. mobile devices password protected). • USB Sticks and iPads – Easily lost. Either use encryption or password protect sensitive files.
6	**Act Fast**	• Timeframes under the regulations are shortening. • Provide documents and deal with data requests promptly. • Pass any requests you are aware of to your Manager/Data Controller as soon as possible.
7	**Beware Viruses & Hacking**	• Don't open emails from recipients you are unsure of. • Ensure machines have anti-virus software.
8	**Better Safe Than Sorry**	• Obligation to notify breaches applies to everyone. • If you are unsure of the potential risk, best to inform your manager. • New technologies - encountering things we don't know. Again if unsure, best to report it. • Don't assume.
9	**Email Etiquette**	• Sending confidential information by email – encryption? • Think twice before sending – sending incorrect information or to the wrong recipient. • Group emails – blind copy (BCC) recipients to avoid sending others personal data (i.e. email addresses).
10	**Data Back Up/ Retention/ Destruction**	• Does data need to be retained? • Alternatively can it be archived/destroyed? • Ensure it is done securely (shredding, confidential waste bins). • Have back-ups in place in case of worst case scenarios.