THE IONA SCHOOL

Data Protection Policy

(Revised April 2018)

Prepared using the following resources

- 2015 DFE publication Information sharing, advice for practitioners providing safeguarding services to children, young people, parents and carers
- Subject access code of practice version 1.2
- Education Act 1996. The EU general data protection regulation 2016/679
- Section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.
- Articles 6 and 9 of the GDPR
- https://www.gov.uk/education/data-collection-and-censuses-for-schools
- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Statement

The Iona School and Nursery collects and uses personal information (referred to in the Data Protection Act as personal data) about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

The school is registered as a Data Controller, with the Information Commissioner's Office (ICO). Details are available on the ICO website.

Purpose

This policy sets out how the school deals with personal information correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored and whether it is held on paper or electronically.

All school staff and governors involved with the collection, use, processing or disclosure of personal data will be aware of their duties and responsibilities and will adhere to this policy.

What is Personal Information/ data?

Personal information or data is information which relates to a living individual who can be identified from that data, or from that data in addition to other information available to them. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

What is Sensitive Personal Data?

Sensitive personal data includes information as to an individual's racial or ethnic origin, their political opinions, religious beliefs or beliefs of a similar nature, whether they are a member of a trade union, their physical or mental health or condition, sexual life, the commission or alleged commission of an offence and any proceedings for an offence committed or alleged to have been committed by them, the disposal of those proceedings or the sentence of any court in such proceedings.

Data Protection Principles

The Data Protection Act 1998 establishes eight principles that must be adhered to at all times:
1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purpose;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data, subject under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
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 data protection.

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

- Inform individuals why personal information is being collected.
- Inform individuals when their information is shared, and why and with whom unless the Data Protection Act provides a reason not to do this.
- Obtain consent before processing Sensitive Personal Data, even if consent is implied within a relevant privacy notice, unless one of the other conditions for processing in the Data Protection Act applies.
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information, known as Subject Access Requests.
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards
- Ensure all staff and governors are aware of and understand these policies and procedures.

<u>Sharing information regarding safeguarding must be read in conjunction with the safeguarding policy</u>

1. Remember that the Data Protection Act 1998 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.

2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice from other practitioners if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible. **The safeguarding lead must always be consulted on sharing children's information.**

4. Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your

judgement, there is good reason to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to be shared.

5. Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.

6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

When and how to share information

When asked to share information, you should consider the following questions to help you decide if and when to share. If the decision is taken to share, you should consider how best to effectively share the information.

When

Is there a clear and legitimate purpose for sharing information?

- Yes – see next question
- No – do not share

Does the information enable an individual to be identified?

- Yes – see next question
- No – you can share but should consider how Is the information confidential?
- Yes – see next question
- No – you can share but should consider how

Do you have consent?

- Yes – you can share but should consider how
- No – see next question

Is there another reason to share information such as to fulfil a public function or to protect the vital interests of the information subject?

- Yes – you can share but should consider how
- No – do not share

How

- Identify how much information to share
- Distinguish fact from opinion
- Ensure that you are giving the right information to the right individual
- Ensure where possible that you are sharing the information securely
- Inform the individual that the information has been shared if they were not aware of this, as long as this would not create or increase risk of harm

All information sharing decisions and reasons must be recorded. If at any stage you are unsure about how or when to share information, you should seek advice and ensure that the outcome of the discussion is recorded. If there are concerns that a child is suffering or likely to suffer harm, then follow the relevant procedures in the safeguarding policy without delay.

For requests for information from parents that may cause harm to either children or staff, this should not be disclosed.

The subject access code of practice (v 1.2) states;

In deciding what information to supply to a SAR you need to have regard to the general principles about exemptions. It is a matter for you to decide whether or not to use an exemption.

Privacy Notice

Why do we collect, share and hold pupil information

Why do we collect and use pupil information? We collect and use pupil information under the Education Act 1996.
The EU general data protection regulation 2016/679 (GDPR) takes effect in May 25 2018
In particular article 6 and 9 of the GDPR
Article 6 GDPR;
Processing is necessary for compliance with a legal duty to which the controller is subjected
Article 9 GDPR ;
for substantial public interest on a legal basis

https://www.gov.uk/education/data-collection-and-censuses-for-schools

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
-

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name and address)
- Any relevant medical information
- Special educational needs
- Exclusions and behavioural information
- Assessment information
- Characteristics (such as ethnicity, language, nationality, country of birth)
- Attendance information (such as sessions attended, number of absences and absence reasons)

Collecting pupil information
Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data
We hold pupil data for until they reach 25years of age.

Who do we share pupil information with?

We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so. We are required to share safeguarding information with the LA and a school the child moves on to.

We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

The School must also comply with an additional condition where it processes special categories of personal information. These special categories are as follows: personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic information, biometric information, health information, and information about sex life or orientation.

Substantial public interest

The processing is necessary for reasons of substantial public interest.

Vital interests:

To protect the vital interests of any person where that person cannot give consent, for example, if they are seriously hurt and are unconscious.

Legal claims:

The processing is necessary for the establishment, exercise or defence of legal claims. This allows us to share information with our legal advisors and insurers.

Medical purposes

This includes medical treatment and the management of healthcare services.

We may ask for your consent to use your information in certain ways. If we ask for your consent to use your personal information you can take back this consent at any time. Any use of your information before you withdraw your consent remains valid.

Requesting access to your personal data

Under data protection legislation, parents have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the school manager

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with the school manager in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Our legal grounds for using your information

This section contains information about the legal basis that we are relying on when handling your information.

Legitimate interests

This means that the processing is necessary for legitimate interests except where the processing is unfair to you. The School relies on legitimate interests for most of the ways in which it uses your information.

Specifically, the School has a legitimate interest in:

- Providing educational services to your child;
- Safeguarding and promoting the welfare of your child (and other children);
- Promoting the objects and interests of the School. This includes fundraising. It also includes making sure that we are able to enforce our rights against you, for example, so that we can contact you if unpaid school fees are due;
- Facilitating the efficient operation of the School; and
- Ensuring that all relevant legal obligations of the School are complied with.

In addition your personal information may be processed for the legitimate interests of others. For example another school will have a legitimate interest in knowing if you have not paid School fees that are due to us.

If you object to us using your information where we are relying on our legitimate interests as explained above please speak to the school manager

Necessary for a contract

We will need to use your information in order to perform our obligations under our contract with you. For example, we need your name and contact details so that we can update you on your child's progress and so that we can contact you if there is a concern.

Legal obligation

Where the School needs to use your information in order to comply with a legal obligation, for example to report a concern to Children's Services. We may also have to disclose your information to third parties such as the courts, the local authority or the police where legally obliged to do so.

Vital interests

For example, to prevent someone from being seriously harmed or killed.

Public interest

The School considers that it is acting in the public interest when providing education.

Issue date

This policy takes effect from April 2010

Review date

This policy will be reviewed and revised by the school manager on an annual basis.

Endorsement

Full endorsement to this policy is given by:

Name:	Mr Martin Taylor
Position:	Iona School Trustee
Signed:	
Date:	12/09/18

Related documents:

- DBS policy
- data protection policy (staff)
- information to outside agencies
- safeguarding