THE IONA SCHOOL & Nursery

Data Protection and handling Data policy for staff

Revised Sept 2018

Prepared using

- **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/**
  - **ICO guidance on security breach management**
  - **DFE Information sharing in Schools and colleges July 2018**
  - **DFE Working together to safeguard children July 2018**
  - **Keeping children safe in education Sept 18**

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.

Sharing information regarding safeguarding must be read in conjunction with the safeguarding policy

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.

The General Data Protection Regulation (GDPR) and Data Protection Act 2018

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 introduce new elements to the data protection regime, superseding the Data

Protection Act 1998. Practitioners must have due regard to the relevant data protection principles which allow them to share personal information,

The GDPR and Data Protection Act 2018 place greater significance on organisations being transparent and accountable in relation to their use of data. All organisations handling personal data need to have comprehensive and proportionate arrangements for collecting, storing, and sharing information.

The GDPR and Data Protection Act 2018 do not prevent, or limit, the sharing of information for the purposes of keeping children and young people safe.

To effectively share information:

- all practitioners should be confident of the processing conditions, which allow them to store, and share, the information that they need to carry out their safeguarding role. Information which is relevant to safeguarding will often be data which is considered 'special category personal data' meaning it is sensitive and personal

- where practitioners need to share special category personal data, they should be aware that the Data Protection Act 2018 includes 'safeguarding of children and individuals at risk' as a condition that allows practitioners to share information **without consent**

- information **can be shared legally without consent**, if a practitioner is unable to, cannot be reasonably expected to gain consent from the individual, or if to gain consent could place a child at risk.

- relevant personal information can be shared lawfully if it is to keep a child or individual at risk safe from neglect or physical, emotional or mental harm, or if it is protecting their physical, mental, or emotional well-being.

Sharing Information

Sharing information is an intrinsic part of any frontline practitioners' job when working with children and young people. The decisions about how much information to share, with whom and when, can have a profound impact on individuals' lives. Information sharing helps to ensure that an individual receives the right services at the right time and prevents a need from becoming more acute and difficult to meet.

Poor or non-existent information sharing is a factor repeatedly identified as an issue in Serious Case Reviews (SCRs) carried out following the death of or serious injury to, a child. In some situations, sharing information can be the difference between life and death.

Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children at risk of abuse or neglect. Every practitioner must take responsibility for sharing the information they hold, and cannot assume that someone else will pass on information, which may be critical to keeping a child safe.

Being alert to signs of abuse and neglect and taking action

All practitioners should be alert to the signs and triggers of child abuse and neglect.[3] Abuse (emotional, physical and sexual) and neglect can present in many different forms.

Indicators of abuse and neglect may be difficult to spot. Children may disclose abuse, in which case the decision to share information is clear, as actions must be taken to respond to the disclosure. In other cases, for example, neglect, the indicators may be more subtle and appear over time. In these cases, decisions about what information to share, and when, will be more difficult to judge. Everyone should be aware of the potential for children to be sexually exploited for money, power, or status, and individuals should adopt an open and inquiring mind to what could be underlying reasons for behaviour changes in children of all ages.

If a practitioner has concerns about a child's safety or welfare, they should share the information with the DSL or the local authority children's social care, or the police, in line with our procedures. Security of information sharing must always be considered and should be proportionate to the sensitivity of the information and the circumstances. If it is thought that a crime has been committed and/or a child is at immediate risk, the police should be notified immediately.

The most important consideration is whether sharing information is likely to support the safeguarding and protection of a child.

Necessary and proportionate

-

When taking decisions about what information to share, you should consider how much information you need to release. Not sharing more data than is necessary to be of use is a key element of the GDPR and Data Protection Act 2018, and you should consider the impact of disclosing information on the information subject and any third parties.
Information must be proportionate to the need and level of risk.

Relevant

Only information that is relevant to the purposes should be shared with those who need it. This allows others to do their job effectively and make informed decisions.

Adequate

Information should be adequate for its purpose. Information should be of the right quality to ensure that it can be understood and relied upon.

Accurate

Information should be accurate and up to date and should clearly distinguish between fact and opinion. If the information is historical then this should be explained.

Timely

Information should be shared in a timely fashion to reduce the risk of missed opportunities to offer support and protection to a child. Timeliness is key in emergency situations and it may not be appropriate to seek consent for information sharing if it could cause delays and therefore place a child or young person at increased risk of harm.
Practitioners should ensure that sufficient information is shared, as well as consider the urgency with which to share it.

Secure

Wherever possible, information should be shared in an appropriate, secure way.

Practitioners must always follow their organisation's policy on security for handling personal information.

Record

Information sharing decisions should be recorded, whether or not the decision is taken to share. If the decision is to share, reasons should be cited including what information has been shared and with whom, in line with organisational procedures. If the decision is not to share, it is good practice to record the reasons for this decision and discuss them with the requester. In line with each organisation's own retention policy, the information should not be kept any longer than is necessary. In some rare circumstances, this may be indefinitely, but if this is the case, there should be a review process scheduled at regular intervals to ensure data is not retained where it is unnecessary to do so.

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. A flowchart follows the text.

When

Is there a clear and legitimate purpose for sharing information?

- Yes – see next question

- No – do not share

Do you have consent to share?

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

Does the information enable an individual to be identified?

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

Have you identified a lawful reason to share information without consent?

- 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
- Where possible, be transparent with the individual, informing them that that the information has been shared, as long as doing so does not create or increase the risk of harm to the individual.

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.

However, it may be appropriate to withhold ;

- information that may cause serious harm to the physical or mental health of the pupil or another individual;
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests;
- information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child.

It is wise to always check with the LADO, the DSL and the ICO as regards sharing information to parents if you are unclear.

WHAT WE DO

- We keep personal information about students, parents and teachers secure and safe.
- We are aware that unauthorised access or loss of information can cause serious harm to people. The ICO can issue fines if they learn that appropriate safety precautions are not being taken.
- We avoid the use of memory sticks completely or ensure they are password protected and fully encrypted.

Security Measures

Currently we carry out the following

- Shredding or incinerating all confidential waste.
- Using strong passwords.
- Installing a firewall and virus checker on computers.
- Pass wording any personal information held electronically.
- Holding telephone calls in private areas.
- Checking the security of storage systems.
- Keeping devices under lock and key when not in use.
- Not leaving papers and devices lying around.
- proper erasing of old hard drives
- pass wording all computers

Emails

- All emails with sensitive or personal data must be encrypted or password protected

Payslips

- Are all sent via an online portal, we no longer store these in paper form or offer them to employees in paper form

Privacy notices

- Are on the school website, in the handbooks and the application forms

Invoices/statements and remittances sent out

- Are password protected

Paper files

- Are kept in locked rooms in locked cabinets, we recognise that this data is still liable to breaches.
- It is important for staff member so realise that the GDPR also relates to this data, as there will be electronically held data that relates to this, for instance, personal files whilst on paper, there will be a link to these.

Computers

- Are all password protected

- accounts packages are on a pass worded PC and are also pass worded with a different password
- Files that contain data are password protected

Cloud storage

- Is done via Livedrive we have contacted them and are reassured that their security is very high

Consent

Under GDPR, consent must be explicitly given to anything that isn't within the normal business of the school, especially if it involves a third party managing the data. Parents (or the pupil themselves depending on their age) must express consent for their child's data to be used outside of the normal business of the school.

Consent is only one of six legal grounds for processing data under the GDPR. Other legal processing conditions are outlined in Article 6 of the GDPR, and conditions for processing 'special categories of data' (i.e. personal data revealing race, ethnicity, political opinions, religion, beliefs or trade union membership, sexual orientation, sex life, and biometric/genetic data used to identify a person) are outlined in Article 9.

Schools only need to obtain consent to process data when they cannot do so under any other lawful basis, such as complying with a regulatory requirement.

For example, consent would not need to be obtained to process data that the school provides to the DfE as part of the census – this is a legal obligation; therefore, the data can be processed lawfully without consent.

Consent would need to be obtained, for example, where the school wishes to collect parents' email addresses to send fundraising and marketing emails to them – there is no other lawful basis to process this data; therefore, consent must be obtained.

<u>we have the following statement on our application and pupil information forms</u>

I understand that my consent is not needed to process data that the school provides under legal obligations; as this can processed lawfully without consent.
I do give my consent for my personal details to be stored in order for the school to use these for their own fundraising and marketing purposes. I understand that I can withdraw my consent at any time.

Please see the data protection policy for further information

We will also obtain separate consent for different processing arrangements. For example, if a parent has consented for their child's picture to be used on the school website, this cannot be used to infer that a parent consents for their child's picture to be used in a school newsletter. We ensure that clear concise consent is given on all subjects. We do not use tick boxes as these can be confusing.

<u>DATA BREACH</u>

WHAT IS A PERSONAL DATA SECURITY BREACH?

A personal data security breach is any event that has the potential to affect the confidentiality, integrity or availability of personal data held by the school or nursery in any format. Personal data security breaches can happen for a number of reasons, including:

- The disclosure of confidential data to unauthorised individuals;
- Loss or theft of portable devices or equipment containing identifiable personal, confidential or sensitive data e.g. PCs, USB, mobile phones; Laptops, disks etc.;
- Loss or theft of paper records;
- Attempts to gain unauthorised access to computer systems, e.g. hacking;
- Records altered or deleted without authorisation from the data "owner"
- Viruses or other security attacks on IT equipment systems or networks;
- Breaches of physical security e.g. forcing of doors on filing cabinet containing confidential information;
- Confidential information left unlocked in accessible areas;
- Insecure disposal of confidential paper waste;
- leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information;
- Publication of confidential data on the internet in error and accidental disclosure of passwords;
- Misdirected emails or faxes containing identifiable personal, confidential

What to do in the case of a data breach

If there is a data breach in any way, this must be recorded on an all incident report form, then given to the data officer (Fiona Stuart) or the acting data officer (Dominique Allen) within 24hours. the form must contain the following

- If a personal data security breach has taken place; if so:
- What personal data is involved in the breach;
- The cause of the breach;
- The extent of the breach (how many individuals are affected);
- The harms to affected individuals that could potentially be caused by the breach; and
- How the breach can be contained.

They will ascertain the risk of the breach using the following scale

Rating	**0**	**1**	**2**	**3**	**4**	**5**	**6**
Reputation	No significant reflection on any individual or body Media interest very unlikely	Damage to an individual's reputation. Possible media interest (eg prominent member of the College /trustee involved)	Damage to a class/office/kg/nursery reputation. Some local or subject specific school media interest that may not go public	Damage to a schools reputation/ Low key local media coverage	Damage to school or nurseries reputation local media coverage.	Damage to school/nursey reputation/ national media coverage.	Monetary Penalty Imposed by ICO
Individuals potentially affected	Minor breach of confidentiality. Only a single individual affected	Potentially serious breach. Less than 5 people affected or risk assessed as low (eg files were encrypted)	Serious potential breach & risk assessed high (eg unencrypted sensitive/health records lost) Up to 20 people affected	Serious breach of confidentiality eg up to 100 people affected and/or identifiable or particularly sensitive ie redundancies, restructuring	Serious breach with either particular sensitivity (eg sexual or mental health details, identifying information of vulnerable people), or up to 1000 people affected	Serious breach with potential for ID theft or over 1000 people affected	Restitution to injured parties Other Liabilities Additional Security Legal Costs

We only have to notify the ICO of a breach it could result in a risk to the rights and freedoms of individuals.

For example if it could result in discrimination, damage to reputation, financial loss or any other significant economic or social disadvantage.

It is compulsory that all data breaches which are likely to have a detrimental effect on the data subject are reported to the ICO within 72 hours. (4,5,6)

We will consider the potential adverse consequences for individuals, i.e. how likely are adverse consequences to materialise and, if so, how serious or substantial are they likely to be. The information provided at Stage 1 on the all incident report form will assist with this stage.

- Assess the risks and consequences of the breach:
    - Risks for individuals:
        - What are the potential adverse consequences for individuals?
        - How serious or substantial are these consequences?
        - How likely are they to happen?
    - Risks for the School /Nursery
        - Strategic & Operational
        - Compliance/Legal
        - Financial
        - Reputational Continuity of Service Levels

- Consider what type of data is involved, how sensitive is it? Were there any protections such as encryption? What has happened to the data? If data has been stolen it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged this poses a different type and level of risk;
- Consider how many individuals' personal data are affected by the breach. It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment;
- Consider the individuals whose data has been breached. Whether they are staff, students, or suppliers will to some extent determine the level of risk posed by the breach and therefore, the actions in attempting to mitigate those risks;
- Consider what harm can come to the affected individuals. Are there risks of physical safety or reputation, of financial loss or a combination?
- Consider if there are wider consequences to consider such as a loss of public confidence in an important service the school provides; and
- Determine, where appropriate, what further remedial action should be taken on the basis of the incident report to mitigate the impact of the breach and prevent repetition.

The investigators will prepare an **incident report** setting out (where applicable):

- a summary of the security breach;
- the people involved in the security breach (such as staff members, students, contractors, external clients);
- details of the information, IT systems, equipment or devices involved in the security breach and any information lost or compromised as a result of the incident;
- how the breach occurred;

- actions taken to resolve the breach;
- impact of the security breach;
- unrealised, potential consequences of the security breach;
- possible courses of action to prevent a repetition of the security breach;
- side effects, if any, of those courses of action; and
- recommendations for future actions and improvements in data protection as relevant to the incident.

Notification

On the basis of the evaluation of risks and consequences, the Lead Investigator in consultation with the college and trustees and others involved in the incident as appropriate, will determine whether it is necessary to notify the breach to others outside the school or nursery. For example:

- the Police
- individuals (data subjects) affected by the breach
- the Information Commissioner's Office
- other bodies such as Department for Employment and Learning
- Our PR company
- the College's insurers
- bank or credit card companies
- trade unions
- external legal advisers

As well as deciding **who** to notify, the Lead Investigator must consider:

- **What** is the message that needs to be put across?

In each case, the notification should include as a minimum:

- a description of how and when the breach occurred;
- what data was involved; and
- what action has been taken to respond to the risks posed by the breach.

When notifying individuals, the Lead Investigator should give specific and clear advice on what steps they can take to protect themselves, what the school is willing to do to assist them and should provide details of how they can contact the school for further information (e.g. helpline, website).

Use of portable devices

The school recognises that personal data may be accessed by users out of school, however, we fully prohibit the use of **memory sticks.**

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage.
- Users must take particular care that laptops which contain personal data must not be accessed by other users (eg family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home),

they should preferably have secure remote access to the management information system or learning platform;

- if secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of data
The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

- The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Burning or shredding is a good way!
- Electronic files must be securely overwritten, in accordance with government guidance and other media such as CD/DVD/Memory sticks must be incinerated or otherwise disintegrated for data, with any references to that deleted off the system. Remember to empty your recycle bin!

A Destruction Log is kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Myth-busting guide

Sharing of information between practitioners and organisations is essential for effective identification, assessment, risk management and service provision. Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children and young people at risk of abuse or neglect. Below are common myths that can act as a barrier to sharing information effectively:

The GDPR and Data Protection Act 2018 are barriers to sharing information

No – the GDPR and Data Protection Act 2018 do not prohibit the collection and sharing of personal information. They provide a framework to ensure that personal information is shared appropriately. In particular, the Data Protection Act 2018 balances the rights of the information subject (the individual whom the information is about) and the possible need to share information about them. Never assume sharing is prohibited – it is essential to consider this balance in every case. You should always keep a record of what you have shared.

Consent is always needed to share personal information

No – you do not necessarily need the consent of the information subject to share their personal information.

Wherever possible, you should seek consent and be open and honest with the individual from the outset as to why, what, how and with whom, their information will be shared.
You should seek consent where an individual may not expect their information to be passed on.
When you gain consent to share information, it must be explicit, and freely given.

There may be some circumstances where it is not appropriate to seek consent, either because the individual cannot give consent, it is not reasonable to obtain consent, or because to gain consent would put a child or young person's safety or well-being at risk.

Where a decision to share information without consent is made, a record of what has been shared should be kept.

Personal information collected by one organisation cannot be disclosed to another organisation

No - this is not the case, unless the information is to be used for a purpose incompatible with the purpose it was originally collected for. In the case of children in need, or children at risk of significant harm, it is difficult to foresee circumstances where information law would be a barrier to sharing personal information with other practitioners.

Practitioners looking to share information should consider which processing condition in the Data Protection Act 2018 is most appropriate for use in the particular circumstances of the case. This may be the safeguarding processing condition or another relevant provision.

The common law duty of confidence and the Human Rights Act 1998 prevent the sharing of personal information

No - this is not the case. In addition to the GDPR and Data Protection Act 2018, practitioners need to balance the common law duty of confidence, and the rights within the Human Rights Act 1998, against the effect on children or individuals at risk, if they do not share the information.

If information collection and sharing is to take place with the consent of the individuals involved, providing they are clearly informed about the purpose of the sharing, there should be no breach of confidentiality or breach of the Human Rights Act 1998. If the information is confidential, and the consent of the information subject is not gained, then practitioners need to decide whether there are grounds to share the information without consent. This can be because it is overwhelmingly in the information subject's interests for this information to be disclosed. It is also possible that a public interest would justify disclosure of the information (or that sharing is required by a court order, other legal obligation or statutory exemption).

In the context of safeguarding a child or young person, where the child's welfare is paramount, it is possible that the common law duty of confidence can be over overcome. Practitioners must consider this on a case-by-case basis. As is the case for all information processing, initial thought needs to be given as to whether the objective can be achieved by limiting the amount of information shared – does all of the personal information need to be shared to achieve the objective?

IT Systems are often a barrier to effective information sharing

No – IT systems, such as the Child Protection Information Sharing project (CP-IS), can be useful in supporting information sharing. IT systems are most valuable when practitioners use the data that has been shared to make more informed decisions about how to support and safeguard a child. Evidence from the Munro Review is clear that IT systems will not be fully effective unless individuals from organisations co-operate around meeting the needs of the individual child. Professional judgment is the most essential aspect of multi-agency work, which could be put at risk if organisations rely too heavily on IT systems.

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:	05/09/18

Related documents:

- DBS policy
- data protection policy staff
- data protection policy pupils and parents
- information to outside agencies
- safeguarding