Personal Data Handling Policy

Perins MAT

Statutory Policy

Policy Updated	March 2019
Next review	Sept 2019
Key Person	P Segal
Approved	TB 3/4/19
Placed on Website	

Introduction

The Perins MAT (which includes our schools, Perins and Sun Hill Junior, our businesses Patchwork Nursery & Pre-School and Evolution Health & Fitness) and its employees (including volunteers, trainees and governors) should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the MAT community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the MAT into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office - for the MAT and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

The DPA lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and correction. The DPA requires organisations to comply with eight data protection principles, which, among others require data controllers to be open about how the personal data they collect is used.

The DPA defines "Personal Data" as data which relate to a living individual who can be identified (http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions)

- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It further defines "Sensitive Personal Data" as personal data consisting of information as to:

- the racial or ethnic origin of the data subject
- his political opinions
- his religious beliefs or other beliefs of a similar nature

- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- his physical or mental health or condition
- his sexual life
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

Guidance for organisations processing personal data is available on the Information Commissioner's Office website: https://ico.org.uk/for-organisations/guide-to-data-protection/

Policy Statements

The MAT will hold the minimum personal data necessary to enable it to perform its functions and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

Personal Data

The MAT and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include but is not limited to:

- Personal information about members of the school communities – including pupils, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular or academic data e.g. class lists, pupil progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Membership and health information for Evolution and Community customers
- Development information for Patchwork children
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Responsibilities

The MAT's Senior Information Risk Officer (SIRO) and Data Protection Officer (DPO) is Phil Segal. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment and make appropriate recommendations to the head teacher, governing body, Trustees and members.
- appoint the Information Asset Owners (IAOs)

Each organisation within the MAT will identify Information Asset Owners (IAOs) for the various types of data being held (e.g. pupil / student information / staff information / assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to protected data and why.

Everyone in the MAT has the responsibility of handling protected or sensitive data in a safe and secure manner.

Members, Trustees and Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in that role.

Registration

The MAT is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. Each school, organisation and business within the MAT is a representative of the MAT for the purposes of data handling.

http://www.ico.org.uk/what_we_cover/register_of_data_controllers.aspx

Information to Staff, Parents / Carers / members etc. – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the MAT informs staff, parents and carers of all pupils of the data they collect, process and hold them, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. The MAT also informs members and customers of the data they collect, process and hold them, the purposes for which the data is held and the third parties (contractors and agencies) to whom it may be passed.

The full Privacy Notice is available on the websites of each of the MAT's organisations.

Training & awareness

All staff will receive data handling awareness and data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners and the Data Protection Officer

Risk Assessments

Data Protection Impact risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of a Data Protection Information Risk Assessment Form

Impact Levels and protective marking *(Schools Data)*

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

Government Protective Marking Scheme label	Impact Level (IL)	Applies to schools?
Not Protectively Marked	0	Will apply in schools
Protect	1 or 2	
Restricted	3	
Confidential	4	Will not apply in schools
Highly Confidential	5	
Top Secret	6	

Most pupil or staff personal data that is used within educational institutions will come under the PROTECT classification. However, some, e.g. the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.

The MAT will ensure that all staff, independent contractors working for it, delivery partners and data processors, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (paper or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g. "Securely delete or shred this information when you have finished using it".

Secure Storage of and access to data

The MAT will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information systems.

All users will use strong passwords which must be changed regularly. User passwords must never be shared. Where available multi-factor authentication will be enforced on external facing systems.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All files containing multiple records or any special category/sensitive data will be password protected. Documents created in Microsoft Office applications all offer encryption by password.

No file containing personal data will be sent to an external recipient without first being password encrypted.

All storage media must be encrypted and stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media, only where the portable media has been approved and encrypted by the MAT's IT staff) Private equipment (i.e. owned by the users) must not be used for the storage of personal data. Private equipment may be used to access MAT data through the provided, secure remote services.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
- the device must be password protected *(many memory sticks / cards and other mobile devices cannot be password protected),*
- the device must offer approved virus and malware checking software *(memory sticks will not provide this facility, most mobile devices will not offer malware protection),* and
- the data must be securely deleted from the device, in line with the MAT data retention policy once it has been transferred or its use is complete.

The MAT has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

The MAT has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Microsoft 365, Google apps and Google Docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The MAT will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. Users must only use cloud storage provided by the MAT and must not upload personal data to their personal cloud storage.

To reduce the risk of inadvertent sharing, any file containing personal information should be stored in the appropriate location on the school's networks (Perins, Sun Hill Junior, Patchwork & Evolution). Files which are resources for use in learning and teaching should be saved to cloud storage and may be shared appropriately.

(see appendix for further information and the ICO Guidance: https://ico.org.uk/your-data-matters/online/cloud-computing/

As a Data Controller, the MAT is responsible for the security of any data passed to a "third party". Data Protection clauses as well as non-disclosure agreements, where appropriate will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material will be held in lockable storage, whether on or off site.

The MAT recognises that under Section 7 of the DPA, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place and detailed in our Data Access Policy to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

The MAT recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the MAT sites or authorised premises without explicit permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when off site
- 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 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. This includes paper and digital data
- 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 requested to be transferred to another country, particularly outside the European Economic Area countries, and advice should be taken from the Data Protection Officer and local authority (if relevant) in this event.**

Disposal of data

The MAT 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, will be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data to ISO27001 /27002.

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

Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals.

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO/DPO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Use of technologies and Protective Marking

	The information	The technology	Notes on Protect Markings (Impact Level)
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Learning and achievement	Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Appendices: Additional issues / documents related to Personal Data Handling in Schools:

Use of Biometric Information

The Protection of Freedoms Act 2012, includes measures that will affect schools and colleges that use biometric recognition systems, such as fingerprint identification and facial scanning:

- We must obtain the written consent of a parent before we take and process a child's biometric data.
- We must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Act 2018.
- We provide alternative means for accessing services where a parent or pupil has refused consent.

Use of Cloud Services

What policies and procedures should be put in place for individual users of cloud-based services?

The school is ultimately responsible for the contract with the provider of the system, so we check the terms and conditions carefully; below is a list of questions that we to consider when selecting a cloud services provider;

- How often is the data backed up?
- Does the service provider have a clear process to recover data?
- Who owns the data stored on the platform?
- How does the service provider protect privacy?
- Who has access to the data?
- Is personal information shared with anyone else?
- Does the service provider share contact details with third party advertisers? Or serve users with ads?
- What steps does the service provider take to ensure that information is secure?
- Is encryption used? Is https used as default or is there an option to use this? Two step verification?
- How will data be protected?
- How reliable is the system?
- What level of support is offered as part of the service?

Parental permission for use of cloud hosted services

As the use of embedded cloud hosting services (Google Aps for Education and Office 365) is part of the MAT schools' core function, we are not required to seek parental permission to set up an account for pupils / students. However, some of the providers themselves have relevant terms and conditions;

Google Apps for Education services - http://www.google.com/apps/intl/en/terms/education_terms.html requires a school to obtain 'verifiable parental consent'. MAT schools will incorporate this into their standard acceptable use

consent forms sent to parents each year (see suggested wording on "Parent / Carer Acceptable Use Agreement Template").

Privacy and Electronic Communications

MAT schools and organisations should be aware that they are subject to the Privacy and Electronic Communications Regulations in the operation of their websites.

Freedom of Information Act

The MAT and all schools (including Academies, which were previously exempt) must have a Freedom of Information Policy which sets out how it will deal with FOI requests. Our FOI policy will:

- Delegate to the Head Teacher day-to-day responsibility for FOIA policy and the provision of advice, guidance, publicity and interpretation of the school's policy
- Consider designating an individual with responsibility for FOIA, to provide a single point of reference, coordinate FOIA and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need
- Consider arrangements for overseeing access to information and delegation to the appropriate governing body
- Proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually
- Ensure that a well-managed records management and information system exists in order to comply with requests
- Ensure a record of refusals and reasons for refusals is kept, allowing the Academy MAT to review its access policy on an annual basis

Model Publication Scheme

Please refer to our Freedom of Information Policy for our publication scheme

Appendix - DfE Guidance on the wording of the Privacy Notice

Privacy Notice - Data Protection Act 1998

We **The Perins Multi Academy Trust** are a data controller for the purposes of the Data Protection Act. Perins Community and Patchwork Nursery are subsidiary representatives of the MAT. We collect information from you and may receive information about you. We hold this personal data and use it to:

- Support your child's development;
- Monitor and report on your child's progress;
- Provide appropriate pastoral care, safety and wellbeing for your child and

- Assess how well our organisation is doing.

This information includes (but may not be limited to) your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information

We will not give information about you to anyone outside the organisation without your consent unless the law and our rules allow us to.

We are required by law to pass some information about you to the Local Authority and the Department for Education (DfE)

If you want to see a copy of the information about you that we hold and/or share, please contact **The Data Protection Officer, The Perins MAT, Perins School, Pound Hill, Alresford SO24 9BS**

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

Hampshire County Council and
http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

data.protection@hants.gov.uk

Public Communications Unit, Department for Education
Sanctuary Buildings
Great Smith Street
London
SW1P 3BT

Website: www.education.gov.uk

Email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288