The Minerva Learning Trust

PERSONAL DATA HANDLING POLICY

Adopted by the Board of Trustees of the Minerva Learning Trust

Minerva Learning Trust	**Kay Taylor, Executive Principal**
Bridport Primary School	**Debbie Brown, Headteacher**
Burton Bradstock CE Primary School	**Claire Staple, Headteacher**
St Mary's CE Primary School	**Helen Farmer, Headteacher**
The Sir John Colfox Academy	**David Herbert, Headteacher**

Policy Written by	**The Minerva Learning Trust**
Ratified by **The Minerva Learning Trust Board**	**9 May 2018**
Date for Review	**May 2021**
Signature of Chair	_____

The Minerva Learning Trust Personal Data Handling Policy

Table of Contents

1. Introduction

1.1
Schools and their employees 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 school 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.

1.2
Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office - for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

1.3
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, e.g. The General Data Protection Regulation (GDPR), 2018.

1.4
This policy must be read in conjunction with following:

- **Acceptable Use of ICT Policy (School policy)**

- **Data Protection Policy**
- **Staff Code of Conduct**
- **Staff Access to Personal Files Policy**

2. Policy Statements

2.1
The Minerva Learning Trust adheres to the principle of Privacy by Design (Ch.4, Art.25, GDPR). It will hold the minimum personal data necessary to enable it to perform its function and not hold it for longer than necessary for the purposes it was collected for.

2.2
Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

2.3
All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Lawfulness for Processing" (Ch.2, Art.26, GDPR).

3. Personal Data

3.1
The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital/biometric format or on paper records. Personal data is defined as any combination of data items that identifies a living individual and provides specific information about them, their families or circumstances. This will include:

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

4. Responsibilities

4.1
The Minerva Learning Trust Data Protection Officer (DPO) is Tracy Broadbent. ICT Manager. The DPO 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.
- maintain a Data Flow and Data Inventory for each Minerva Learning Trust school to establish information pathways and minimise risk.
- report to the Executive Principal.
- monitor data protection compliance in MLT schools.
- advise as required on Data Protection Impact Assessments.
- co-operate with the supervisory authority, Information Commissioner's Office (ICO).
- have due regard for the risk associated with processing, taking account of the nature, scope and context of processing.

4.2
Executive Principal

- Responsible for ensuring data protection incidents are reported to the Information Commissioner's Office (ICO);
- Co-operate with the supervisory authority, ICO;
- Monitor the DPO;
- Ensure the DPO is able to carry out their responsibilities effectively and without interference;

4.2
Head Teacher

- Responsible for ensuring all senior staff and the school are compliant with the General Data Protection Regulation;
- Provide guidance to ensure all staff are aware of their data protection responsibilities under the regulation;
- Responsible for managing and reporting data breaches to the Minerva Learning Trust Data Protection Officer or Executive Principal;
- Provide guidance to process Subject Access and Freedom of Information Requests;
- Ensure staff are compliant with this policy and associated procedures.

4.3
All Staff

- Responsible for handling protected or sensitive data in a safe and secure manner;
- Responsible for reporting data breaches to the Head Teacher or DPO.

4.4
Members, Trustees and Governors

- Must comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Trustee or Governor.

5. Registration

5.1
The Minerva Learning Trust is registered as a Data Controller on the Data Protection Register held by the Information Commissioner (Registration number ZA112950).

6. Information to Parents / Carers – the "Privacy Notice"

6.1
In order to comply with the fair processing requirements of the GDPR, the school will inform parents / carers of all pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc.) to whom it may be passed. This privacy notice will be passed to parents / carers through each Minerva Trust school website and is on display in each school.

7. Training & awareness

7.1
All staff will receive data handling awareness / 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 the SLT and DPO

8. Privacy Impact Assessments

8.1
Privacy Impact Assessments (PIAs) will be carried out by the DPO to establish the security measures already in place and whether they are the most appropriate and cost effective. PIAs will also be carried out prior to any new electronic or manual procedure for collecting, storing and sharing data is implemented. The PIA will involve:

- Prioritising the rights and freedoms of data subject;
- Recognising the risks/vulnerabilities that are present;
- Judging the level of the risks (both the likelihood of and consequences to the data subject); and
- Prioritising the risks.

8.2
Risk assessments are an ongoing process and should always result in the completion of a PIA

9. Impact Levels and protective marking

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	

9.1
The school will ensure that all school staff, independent contractors working for it, and delivery partners, 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.

9.2
All documents (manual 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.

9.3
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 students / 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.

9.4
Release and destruction markings should be shown in the footer e.g. "Securely delete or shred this information when you have finished using it".

10. Secure Storage of and access to data

10.1
The Minerva Learning Trust 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 system.

10.2
All users will use strong passwords. User passwords must never be shared.

10.3
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.

10.4
All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

10.5
Personal data can only be stored on school equipment (this includes computers and portable storage media. Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

10.6
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,
- the device must offer approved virus and malware checking software, and
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

10.7
The Minerva Learning Trust has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

10.8
The Minerva Learning Trust has clear policy and procedures for the use of “Cloud Based Storage Systems” (for example, Microsoft 365, Bromcom and MyConcern) and is aware that data held in remote and cloud storage is still required to be protected in line with the General Data Protection Regulation 2018. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data and that a PIA is carried out to assess risk.

10.9
As a Data Controller, the Minerva Learning Trust is responsible for the security of any data passed to a “third party”. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

10.10

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

10.11
The Minerva Learning Trust recognises that under Chapter 3 of the GDPR, data subjects have a number of rights in connection with their personal data, including the right of access. Procedures are in place (Data Subject Access Request Information, Access to Personal Data Request) to deal with Subject Access Requests i.e. an oral or 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. The data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

11. Secure transfer of data and access out of school

11.1
The Minerva Learning Trust 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 school or authorised premises without 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 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 have secure remote access to the management information system or learning platform i.e. via a unique, secure password;
- 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 DPO (if relevant) in this event in relation to Chapter 5 of the GDPR.

12. Disposal of data

12.1
The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

12.2
The disposal of personal data, in either paper or electronic form, must 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.

12.3

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

13. Audit Logging / Reporting / Incident Handling

13.1
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 DPO will keep a Data Flow and Data Inventory that documents these activities.

13.1
Audit logs will be kept providing evidence of accidental or deliberate data security breaches of electronic, manual, biometric and CCTV data – including loss of protected data or breaches of an Acceptable Use Policy and the Staff Code of Conduct. Incidents should be reported as soon as a member of staff becomes aware of them to the Headteacher in each Minerva Trust school, who will fill in a Data Incident Report.

13.1
The Data Incident Report (for reporting, managing and recovering from information risk incidents) 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.

13.1
All significant data protection incidents must be reported through the Executive Principal/DPO to the Information Commissioner's Office within 72 hours of becoming aware of the breach.

Appendix A

Use of technologies and Protective Marking

The following provides a useful guide:

	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 school closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.