Villa Real School

together we achieve

Data Protection Policy

Responsibility: Louise Burns Date: March 2021

Adopted by the Governing Body:

Chair of Governors

Date: 24.05.2021

Date to be reviewed: March 2022

Data Protection Policy
RRSA Article Links.

Article 16. Right to Privacy.
Every child has the right to privacy. The law should protect the child's private, family and home life.

AIMS AND OBJECTIVES

The aim of this policy is to provide a framework to enable staff, parents/ carers and pupils/ students at Villa Real School to understand:

- the law regarding personal data
- how personal data should be processed, stored, archived and disposed of
- how staff, parents/ carers and pupils/ students can access personal data
- the rights in respect of people whose data is being held and processed by the school (this includes pupils/ students, parents/ carers, staff and governors)

The Data Protection Act 2018 and GDPR do not prevent, or limit, the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children.
Keeping children safe in Education
https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

IT IS A STATUTORY REQUIREMENT FOR ALL SCHOOLS TO HAVE A DATA PROTECTION POLICY

In addition to this policy, Villa Real School has the following policies:

Retention Information - details on how long all records are retained
Information Asset Audit - a comprehensive audit listing all the information that the school holds, who has access to the information and the legal basis for processing it
Privacy Notices - for pupils/students, parents, staff and governors
Transfer of Records Policy – for staff
Deletion of data Policy – for staff
Subject Access Policy – for staff, pupils/students, parents/ carers and governors
CCTV Policy - – for staff, pupils/students, parents/ carers and governors

Villa Real School is registered with the ICO and Louise Burns is registered as the DPO.

DATA PROTECTION PRINCIPLES

Article 5 of the GDPR sets out that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, subject to measures respecting the principle of 'data minimisation', not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals, and again subject to the 'data minimisation' principle; and
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition, article 5(2) requires that the data controller shall be responsible for, and be able to demonstrate, compliance with the principles. In effect, we the school, as the 'data controller', need to be able to show that our policies and systems comply with requirements of GDPR.

DATA PROTECTION PRINCIPLES

Article 5 of the GDPR sets out that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, subject to measures respecting the principle of 'data minimisation', not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals, and again subject to the 'data minimisation' principle; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition, Article 5(2) requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles. In effect the school, as the 'data controller', needs to be able to show that its policies and systems comply with requirements of GDPR.

LAWFUL BASIS FOR PROCESSING DATA

GDPR stipulates that there must be a lawful basis for processing data, and that for **special category data** an additional condition has to be met. The vast majority of information that our school collects and processes is required to enable us to perform tasks carried out in the public interest or in the exercise of official authority vested in the school, as the data controller. This is the main lawful basis for processing data that a school is likely to rely on.

There are other bases that may be available, such as a specific legal obligation applying to the data controller that makes the processing necessary:

AGE

Children under the age of 14 are not considered able to give consent to process data or to directly access the rights of a data subject, so parents / carers do this on their behalf. Over the age of 14 this responsibility is transferred to the child and parents/ carers will not have responsibility for their child's data. (This is subject to the Data Protection Bill becoming law. The 'default' age under the GDPR is 16.)

CONSENT

If there is a lawful basis for collecting data, then consent to collect data is not required. (An employee could not opt to withhold an NI number for example.) However, a privacy notice which explains to data subjects (or the parents/ carers of the data subject if under the age of 14) will be required. This explains the lawful basis for processing the data, and also explains to the individual their rights.

Parents/Carers or children over the age of 14 will need to give consent when there is not a legal reason for processing, for instance for images used in school publicity or social media feeds. The consent will need to be transparent, revocable, and will need to be on an "Opt-in" basis.

RIGHTS

The GDPR creates some new rights for individuals and strengthens some existing ones. It provides for the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

For "privacy notices" covering the right to be informed, please see section 5 below.

Different rights attach to different lawful bases of processing:

	Right to erasure	Right to portability	Right to object
Vital Interests	✓	**X**	**X**
Legal Obligation	X	**X**	**X**
Public Task	**X**	**X**	✓
Legitimate Interests	✓	**X**	✓
Contract	✓	✓	**X**
Consent	✓	✓	X but right to withdraw consent

THE RIGHT TO ERASURE

GDPR includes a right to erasure – but this is not an absolute right and does not necessarily override the lawful basis for continuing to hold data. Schools' data management systems such as SIMS will begin to improve their functionality to either delete or anonymise personal data when appropriate. It can be seen from the table above that where the school relies on either a 'legal obligation' or a 'public task' basis for processing (see above) there is no right to erasure – however this does not mean the data will never be erased. It will still not be retained for any longer than necessary, in accordance with statutory requirements and/or the school's data retention guidelines.

DATA TYPES

Not all data needs to be protected to the same standards - the more sensitive or potentially damaging the loss of the data is, the better it needs to be secured. There is inevitably a compromise between usability of systems and working with data. In a school environment staff are used to managing risk, for instance during a PE or swimming lesson where risks are assessed, controlled and managed. A similar process should take place with managing school data. GDPR defines different types of data and prescribes how it should be treated.

The loss or theft of any Personal Data is a "Potential Data Breach" which could result in legal action against the school. The loss of sensitive, or "special category", personal data is considered much more seriously and the sanctions may well be more punitive.

PERSONAL DATA
As a school we 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 includes:

- 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, 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, disciplinary records and references
- Any other information that might be disclosed by parents/ carers or by other agencies working with families or staff members

SPECIAL CATEGORY DATA
"Special Category Data" (information revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership), and the processing of genetic data, biometric data, or data concerning a person's health or sexual life is prohibited except in special circumstances.

This is because special category data is more sensitive, and so needs more protection. In a school, the most likely special category data is:

- information on the racial or ethnic origin of a pupil or member of staff
- information about the sexuality of a child, his or her family or a member of staff
- medical information about a child or member of staff
- Information regarding SEND
- some information regarding safeguarding will also fall into this category
- Staffing information e.g. Staff Trade Union details

TYPES OF DATA NOT COVERED BY THE ACT
This is data that does not identify a living individual and, therefore, is not covered by the remit of the DPA. This may fall under other 'access to information' procedures. This would include lesson plans (where no individual pupil is named), teaching resources, and other information about the school which does not relate to an individual. Some of this data would be available publicly (for instance the diary for the forthcoming year), and some of this may need to be protected by the school (if the school has written a detailed

scheme of work that it wishes to sell to other schools). Schools may choose to protect some data in this category but there is no legal requirement to do so.

The ICO provides additional information on their website. See http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

RESPONSIBILITIES
The Headteacher and Governing Body are responsible for Data Protection. They should appoint a Data Protection Officer to manage data.

RISK MANAGEMENT – ROLES: *Data Protection Officer Louise Burns*
Villa Real School has a nominated member of staff responsible for the management of data protection.

In accordance with the ICO this role includes:

- informing and advising the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments; training staff and conducting internal audits
- being the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc)

RISK MANAGEMENT - STAFF AND GOVERNOR RESPONSIBILITIES
- Everyone in school has the responsibility of handling personal information in a safe and secure manner
- Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor
- Staff should ensure that any information that they provide the school in connection with their employment is accurate and up to date
- Staff must inform the school of any change of address, either at the time of appointment or subsequently. The school cannot be held responsible for any errors unless the staff member has informed the school of such changes
- As part of staff responsibilities, staff are required to collect information about other people: ability, opinions, academic institutions, references and so on. These circumstances require the staff to comply with the new GDPR

LEGAL REQUIREMENTS

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner and each school is responsible for their own registration:
http://ico.org.uk/for_organisations/data_protection/registration
The CCTV is registered with the ICO.

Information for Data Subjects (Parents, Staff): PRIVACY NOTICES

In order to comply with the fair processing requirements of the DPA, the school **must** inform parents/ carers of all pupils / students and staff of the data they collect, process and hold on the pupils / students, the purposes for which the data is held, the legal basis for holding it and the third parties (e.g. LA, DfE, etc.) to whom it may be passed. The privacy notice will also need to set out the data subjects' rights under the GDPR. This privacy notice will be passed to parents/ carers through a letter.

New privacy notices have been issued to all 'data subjects' in 2018 even if the data subject has previously received a similar notice. This is because of the new rights in the GDPR that people should be informed about.

TRANSPORTING, STORING AND DISPOSING OF PERSONAL DATA

Information security - Storage and Access to Data

The more sensitive the data the more robust the security measures that need to be in place to protect it.

Technical Requirements

- The school will ensure that ICT 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
- 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 storage media must be 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 (where allowed). Private equipment (i.e. owned by the users) must not be used for the storage of personal data
- The school has a clear policy and procedures for the automatic backing up, accessing and restoring of all data held on school systems, including off-site backups

Portable Devices

- no use of USB drives or memory cards at all
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete
- Office 365 must be used to store information accessible through the secure cloud

Passwords

- All users will use strong passwords which must be changed regularly. User passwords must never be shared. Do not remember passwords
- Staff must not approve for systems to remember passwords.
- Staff must only log on to school computers and systems using their own log-in accounts. When leaving the work stations all accounts should be closed.

Images

- Images of pupils/ students will only be processed on the school premises and permission for this will be obtained in the photographic permission notice
- Images will be protected and stored in a secure area, such as Office 365
- No photographs of pupils/ students should leave the school unless with the permission of the Head Teacher

Cloud Based Storage

- The school has a clear policy and procedures for the use of "Cloud Based Storage Systems" (e.g. One drive) 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 school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. See advice from the DfE below:- https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

THIRD PARTY DATA TRANSFERS

As a Data Controller, the school 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 as well as data processing agreements.
http://ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

RETENTION OF DATA

- The guidance given by the Information and Records Management Society – Schools records management toolkit will be used to determine how long data is retained
- Personal data that is no longer required will be destroyed and this process will be recorded

SYSTEMS TO PROTECT DATA

Paper Based Systems

- All paper based personal data will be protected by appropriate controls, for example:
    - Paper based personal information sent to parents/ carers (will be checked by office staff before the envelope is sealed).

- Diaries will be double checked by class staff each night to ensure they go home with the correct child
- All letter containing personal data will be sent out via royal mail
- No papers with personal information of pupils/students will leave the school site. This includes the Red Files.

School Websites

Uploads to the school website will be checked prior to publication, for instance:

- to check that appropriate photographic consent has been obtained
- to check that the correct documents have been uploaded

E-mail

- Durham County Council email is a secure email address and suitable for transferring sensitive information

DATA SHARING

The school is required by law to share information with the LA and DfE. Further details are available at: https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

Durham Local Safeguarding Board (DSCP)also provides information on information sharing at: http://www.durham-scp.org.uk/wp-content/uploads/sites/29/2016/06/Guide-for-professionals-on-information-sharing.pdf

Schools should ensure that, where special category data is shared, it is transmitted securely for instance by secure e-mail or is transferred in tamper proof envelopes securely delivered to the recipient.

SAFEGUARDING

Schools MUST follow the statutory processes in Keeping Children safe in Education and Working together to Safeguard Children https://www.gov.uk/government/publications/working-together-to-safeguard-children--2

Durham Local Safeguarding Board (DSCP) provides information on information sharing at: http://www.durham-scp.org.uk/wp-content/uploads/sites/29/2016/06/Guide-for-professionals-on-information-sharing.pdf

TRANSFER OF SAFEGUARDING AND SEND RECORDS WHEN A PUPIL MOVES SCHOOL

The following is an extract from keeping Children safe in Education Sept 2018.

Where children leave the school or college, the designated safeguarding lead should ensure their child protection file is transferred to the new school or college as soon as possible, ensuring secure transit, and confirmation of receipt should be obtained. For schools, this should be transferred separately from the main pupil file.

Villa Real has a separate policy for the Transfer of files.

DATA BREACH – PROCEDURES

On occasion, personal data may be lost, stolen or compromised. The data breach includes both electronic media and paper records, and it can also mean inappropriate access to information.

- In the event of a data breach the data protection officer will inform the head teacher and chair of governors
- The school will follow the procedures set out in Data Breach Policy

This policy will be reviewed, and updated if necessary every two years or when legislation changes.

DATA TRANSFER AFTER BREXIT

At the end of the transition period there will be 2 sets of rules for us to consider:

- UK rules on transferring data outwards from the UK to the EU (including the EEA) and the rest of the world
- The impact of EU transfer rules on those sending you personal data from outside the UK (including from the EEA) into the UK

In both cases, we, as a school, can transfer personal data, if it is covered by an adequacy decision, an appropriate safeguard or an exception.

When sharing data with the EU, Iceland, Liechtenstein and Norway :

We must contact anyone we share personal data with within the EU, Iceland, Liechtenstein or Norway.

We should explain we can still share personal data lawfully with them now that the UK has left the EU.

When receiving data from the EU, Iceland, Liechtenstein and Norway

We must identify where we receive data from the EU, Iceland, Liechtenstein, or Norway, and determine:

- who the data controllers and processors are
- where the data is stored

Appendix 1 - Links to resources and guidance

ICO Guidance on GDPR
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

http://ico.org.uk/for_organisations/sector_guides/education
Specific information for schools is available here. This includes links to guides from the DfE

http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv
Specific Information about CCTV

Information and Records Management Society – Schools records management toolkit
http://irms.org.uk/page/SchoolsToolkit
A downloadable schedule for all records management in schools

Disclosure and Barring Service (DBS)
https://www.gov.uk/government/publications/handling-of-dbs-certificate-information/handling-of-dbs-certificate-information
Details of storage and access to DBS certificate information.

DFE Privacy Notices
https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

DFE Use of Biometric Data
https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

Appendix 2 - Privacy Notices

These are a separate attachment

Appendix 3 - Glossary

GDPR - The General Data Protection Regulation. These are new European-wide rules that are the basis of data protection legislation. They are enforced in the UK by the ICO.

Data Protection Act 1998: Now superseded by GDPR
All personal data which is held must be processed and retained in accordance with the eight principles of the Act and with the rights of the individual. Personal data must not be kept longer than is necessary (this may be affected by the requirements of other Acts in relation to financial data or personal data disclosed to Government departments). Retention of personal data must take account of the Act, and personal data must be disposed of as confidential waste. Covers both personal data relating to employees and to members of the public.

ICO:
The Information Commissioner's Office. This is a government body that regulates the Data Protection Act and GDPR
The ICO website is here http://ico.org.uk/

Data Protection Act 1998: Compliance Advice. Subject access – Right of access to education records in England:
General information note from the Information Commissioner on access to education records. Includes timescale (30 days) and photocopy costs.

Data Protection Act 1998: Compliance Advice. Disclosure of examination results by schools to the media:
General information note from the Information Commissioner on publication of examination results.

Education Act 1996:
Section 509 covers retention of home to school transport appeal papers. (By LA)

Education (Pupil Information) (England) Regulations 2005:
Retention of Pupil records

Health and Safety at Work Act 1974 & Health and Safety at Work Act 1972:
Retention requirements for a range of health and safety documentation including accident books, H&S manuals etc.

School Standards and Framework Act 1998:
Retention of school admission and exclusion appeal papers and other pupil records.

Appendix 4 - Check Sheet

Schools may find it beneficial to use this to check their systems for handling data.

1. Data protection Officer in place
2. Information asset log complete
3. School able to demonstrate compliance with GDPR
4. Training for staff on Data Protection, and how to comply with requirements
5. Data Protection Policy in place
6. All portable devices containing personal data are encrypted
7. Passwords – Staff use complex passwords
8. Passwords – Not shared between staff
9. Privacy notice sent to parents/ carers and pupils/ students aged 13 or over
10. Privacy notice given to staff
11. Images stored securely
12. School registered with the ICO as a data controller
13. Systems in place to ensure that data is retained securely for the required amount of time
14. Process in place to allow for subject access requests
15. If school has CCTV, appropriate policies are in place to cover use, storage and deletion of the data, and appropriate signage is displayed
16. Paper based documents secure
17. Electronic backup of data both working and secure
18. Systems in place to help reduce the risk of a data breach *e.g. personal data sent out checked before the envelope sealed, uploads to websites checked etc*.