

# Data Protection and Retention Policy

## 1. Introduction

This Policy sets out the obligations of Villiers Park Educational Trust ("Villiers Park" or "the Trust") regarding data protection and the rights of individuals, including current employees, interns and volunteers, ex-staff members, current students, previous students ('alumni'), prospective staff members, prospective students, tutors, supporters (donors and fundraisers), trustees and suppliers ("all the aforementioned are data subjects"), in respect of their personal data under the General Data Protection Regulation ("the Regulation") and Privacy and Electronic Communications Regulation (PECR).

The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by Villiers Park, its employees, agents, contractors, interns, volunteers or other parties working on behalf of the Trust.

Villiers Park is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

## 2. The Data Protection Principles

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

- a) processed lawfully, fairly and in a transparent manner in relation to the data subject;
- 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 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 it is processed;
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is 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 is 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 Regulation in order to safeguard the rights and freedoms of the data subject;

- 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.

### **3. Lawful, Fair, and Transparent Data Processing**

The Regulation seeks to ensure that personal data is processed lawfully, fairly and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

- a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- d) processing is necessary to protect the vital interests of the data subject or of another natural person;
- e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
- f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

### **4. Processed for Specified, Explicit and Legitimate Purposes**

#### 4.1

Villiers Park collects and processes the personal data set out in Part 18 of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and data received from third parties (for example, where schools nominate a pupil for our Scholars Programme).

#### 4.2

Villiers Park only processes personal data for the specific purposes set out in Part 18 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected (by directing them to our Privacy Policies and Cookies Policy on our website at <https://www.villierspark.org.uk/>), where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

### **5. Adequate, Relevant and Limited Data Processing**

Villiers Park will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4 above.

### **6. Accuracy of Data and Keeping Data Up To Date**

Villiers Park shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular

intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

## **7. Timely Processing and Data Retention**

Villiers Park shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

## **8. Secure Processing**

Villiers Park shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 19 and 20 of this Policy. (Also please see our IT & Computer Use Policy).

## **9. Accountability**

### 9.1

The Trustees of Villiers Park Educational Trust are responsible for ensuring that appropriate policies and procedures are implemented to ensure the compliance of its data processing activities.

### 9.2.

The Trustees delegate the duties of the Data Controller to the Chief Executive Officer and in his/her absence, to the Senior Leadership Team. Data protection is a standing item on the risk register, reviewed quarterly by the Senior Leadership Team and Board of Trustees.

### 9.3

Villiers Park shall keep records of all personal data collection, holding, and processing, which shall incorporate the following information:

- a) The name and details of Villiers Park, and any applicable third party data controllers;
- b) The purposes for which Villiers Park processes personal data;
- c) Details of the categories of personal data collected, held, and processed by Villiers Park; and the categories of data subject to which that personal data relates (Please see Appendix A for our Data Asset Inventory Schedule);
- d) Details (and categories) of any third parties that will receive personal data from Villiers Park;
- e) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- f) Details of how long personal data will be retained by Villiers Park (Please see Appendix B for our Retention Table); and
- g) Detailed descriptions of all technical and organisational measures taken by Villiers Park to ensure the security of personal data.

## **10. Privacy Impact Assessments**

Villiers Park shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by the Trust's Data Controller and shall address the following areas of importance:

10.1

The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;

10.2

Details of the legitimate interests being pursued by Villiers Park;

10.3

An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

10.4

An assessment of the risks posed to individual data subjects; and

10.5

Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation (Please see Appendix C for a copy of our Privacy Impact Assessment Template).

## **11. The Rights of Data Subjects**

The Regulation sets out the following rights applicable to data subjects:

- a) The right to be informed;
- b) The right of access;
- c) The right to rectification;
- d) The right to erasure (also known as the 'right to be forgotten');
- e) The right to restrict processing;
- f) The right to data portability;
- g) The right to object;
- h) Rights with respect to automated decision-making and profiling.

## **12. Keeping Data Subjects Informed**

12.1

- a) Villiers Park shall ensure that the following information is provided, through reference to its Privacy Policies, to every data subject when personal data is collected:
- b) Details of the Trust and contact details for any queries about the Trust's policy on data collection and processing;
- c) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 18 of this Policy) and the legal basis justifying that collection and processing;
- d) Where applicable, the legitimate interests upon which Villiers Park is justifying its collection and processing of the personal data;
- e) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- f) Where the personal data is to be transferred to one or more third parties, details of those parties;

- g) Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place;
- h) Details of the length of time the personal data will be held by Villiers Park (or, where there is no predetermined period, details of how that length of time will be determined);
- i) Details of the data subject's rights under the Regulation;
- j) Details of the data subject's right to withdraw their consent to Villiers Park's processing of their personal data at any time;
- k) Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);
- l) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;
- m) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

## 12.2

The information set out above in Part 12.1 shall be provided to the data subject at the following applicable time:

- a) Where the personal data is obtained from the data subject directly, at the time of collection via the relevant Privacy Policy available on our website;
- b) Where the personal data is not obtained from the data subject directly (e.g. from another party when Joint Data Controller Agreements or Data Processor Agreements are in place with third parties), within one month of receiving the personal data;
- c) If the personal data is used to communicate with the data subject, at the time of the first communication; or
- d) If the personal data is to be disclosed to another party, before the personal data is disclosed; or
- e) In any event, not more than one month after the time at which Villiers Park obtains the personal data.

## **13. Data Subject Access**

### 13.1

A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which Villiers Park holds about them. Villiers Park is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension). Please see Appendix D for the Trust's Subject Access Request policy and procedures.

### 13.2

All subject access requests should be addressed to the Data Controller, Villiers Park Educational Trust at the postal address: Villiers Park Education Trust, Allia Future Business Centre, King's Hedges Road, Cambridge, CB4 2HY.

### 13.3

Villiers Park does not charge a fee for the handling of normal SARs. The Trust reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

#### **14. Rectification of Personal Data**

##### 14.1

If a data subject informs Villiers Park that personal data held by Villiers Park is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt of the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

##### 14.2

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

#### **15. Erasure of Personal Data**

##### 15.1

Data subjects may request that Villiers Park erases the personal data it holds about them in the following circumstances:

- a) It is no longer necessary for Villiers Park to hold that personal data with respect to the purpose for which it was originally collected or processed;
- a) The data subject wishes to withdraw their consent to Villiers Park holding and processing their personal data;
- b) The data subject objects to Villiers Park holding and processing their personal data (and there is no overriding legitimate interest to allow Villiers Park to continue doing so) (see Part 17 of this Policy for further details concerning data subjects' rights to object);
- c) The personal data has been processed unlawfully;
- d) The personal data needs to be erased in order for Villiers Park to comply with a particular legal obligation

##### 15.2

Unless Villiers Park has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

##### 15.3

In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

#### **16. Restriction of Personal Data Processing**

##### 16.1

Data subjects may request that Villiers Park ceases processing the personal data it holds about them. If a data subject makes such a request, Villiers Park shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

## 16.2

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

## **17. Objections to Personal Data Processing**

### 17.1

Data subjects have the right to object to Villiers Park processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

### 17.2

Where a data subject objects to Villiers Park processing their personal data based on its legitimate interests, the Trust shall cease such processing forthwith, unless it can be demonstrated that Villiers Park's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

### 17.3

Where a data subject objects to Villiers Park processing their personal data for direct marketing purposes, Villiers Park shall cease such processing forthwith.

### 17.4

Where a data subject objects to Villiers Park processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. Villiers Park is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

## **18. Personal Data**

The personal data that may be collected, held, and processed by Villiers Park includes:

- a) First name, second name, date of birth, name of school, home address, school address, phone numbers, health details, school contact details, e-mail address, next of kin contact details, parents'/guardian's contact details, photographs and records of educational achievements from students / prospective students;
- b) First name, second name, passport copy, immigration status, National Insurance number, P45/P46/P60 forms, professional/educational records, references, home address, phone number, e-mail address, next of kin and protected characteristics from prospective/current staff members including employees, interns and volunteers and bank details of current staff;
- c) First name, second name, company address, company phone number, bank details for payments to contractors, suppliers and agents;
- d) First name, second name, e-mail address, home address, phone number, job details, bank details and donation records of current/previous donors/fundraisers/supporters;

- e) First name, second name, job title (position), organisation address, organisation e-mail address and organisation phone number of contact persons in funding organisations and potential funding organisations, and of contact persons who could lead to relationships with major donors, corporate donors or charitable trusts and foundations.

## **19. Data Protection Measures**

Villiers Park shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

- a) All emails containing personal data must be encrypted;
- b) Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded.
- c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- d) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- f) Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- g) Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or posted in a securely sealed envelope;
- h) No personal data may be shared informally and if an employee, intern, volunteer, agent, subcontractor, or other party working on behalf of Villiers Park requires access to any personal data that they do not already have access to, such access should be formally requested from the Chief Executive.
- i) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;
- j) No personal data may be transferred to any employees, interns, volunteers, agents, contractors, or other parties, whether such parties are working on behalf of Villiers Park or not, without the authorisation of the Chief Executive. This permission is deemed granted by following the authorised policies and procedures of the Trust and the arrangements of appropriate data sharing agreements with third parties;
- k) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, interns, volunteers, agents, sub-contractors or other parties at any time;
- l) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
- m) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to Villiers Park or otherwise without formal written approval and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.
- n) No personal data should be transferred to any device personally belonging to an employee, intern or volunteer and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of



Villiers Park where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to Villiers Park that all suitable technical and organisational measures have been taken);

- o) All personal data stored electronically should be encrypted and backed up on a daily basis with back-ups stored offsite.
- p) All electronic copies of personal data should be stored securely using passwords and data encryption;
- q) All passwords used to protect personal data should be selected in accordance with the Password Policy as embedded in the Trust's IT & Computer Use Policy;
- r) Under no circumstances should any passwords be written down or shared between any employees, interns, volunteers, agents, contractors, or other parties working on behalf of Villiers Park, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method;
- s) Where personal data held by Villiers Park is used for Fundraising and Communications purposes, it shall be the responsibility of the Director of Fundraising to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service and other platforms such as Social Media accounts and SMS. Such details should be checked at least annually.

## **20. Data Protection Measures**

Villiers Park shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

- a) All emails containing personal data must be encrypted;
- b) Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded.
- c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- d) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- f) Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- g) Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or posted in a securely sealed envelope;
- h) No personal data may be shared informally and if an employee, intern, volunteer, agent, subcontractor, or other party working on behalf of Villiers Park requires access to any personal data that they do not already have access to, such access should be formally requested from the Chief Executive.
- i) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;
- j) No personal data may be transferred to any employees, interns, volunteers, agents, contractors, or other parties, whether such parties are working on behalf of Villiers Park or not, without the authorisation of the Chief Executive. This permission is deemed granted by following the authorised policies and procedures

- of the Trust and the arrangements of appropriate data sharing agreements with third parties;
- k) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, interns, volunteers, agents, sub-contractors or other parties at any time;
  - l) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
  - m) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to Villiers Park or otherwise without formal written approval and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.
  - n) No personal data should be transferred to any device personally belonging to an employee, intern or volunteer and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Villiers Park where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to Villiers Park that all suitable technical and organisational measures have been taken);
  - o) All personal data stored electronically should be encrypted and backed up on a daily basis with back-ups stored offsite.
  - p) All electronic copies of personal data should be stored securely using passwords and data encryption;
  - q) All passwords used to protect personal data should be selected in accordance with the Password Policy as embedded in the Trust's IT & Computer Use Policy;
  - r) Under no circumstances should any passwords be written down or shared between any employees, interns, volunteers, agents, contractors, or other parties working on behalf of Villiers Park, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method;

Where personal data held by Villiers Park is used for Fundraising and Communications purposes, it shall be the responsibility of the Director of Fundraising to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service and other platforms such as Social Media accounts and SMS. Such details should be checked at least annually.

## **21. Data Breach Notification**

### 21.1

All personal data breaches must be reported immediately to Villiers Park's Chief Executive.

### 21.2

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), Villiers Park must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

### 21.3

In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 21.2) to the rights and freedoms of data subjects, the Trust's Data Controller must ensure that all affected data subjects are informed of the breach directly and without undue delay.

#### 21.4

Data breach notifications shall include the following information:

- a) The categories and approximate number of data subjects concerned;
- b) The categories and approximate number of personal data records concerned;
- c) The name and contact details of the Trust's Chief Executive (or other contact point where more information can be obtained);
- d) The likely consequences of the breach;
- e) Details of the measures taken, or proposed to be taken, by Villiers Park to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

## **22. Implementation of Policy**

This Policy was updated in June 2022, and originally implemented and effective as of May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy was approved by the Trustees of Villiers Park Educational Trust at their Board meeting on 20th July 2022.

Approved on 20 July 2022

Authorised by

Related Policies

Privacy Policy (available on our website)

Job Applicant Privacy Notice (available on our website)

Employee Handbook Section 15 – Information Technology & Computer Use Policy

Employee Handbook Section 31 – Employee Privacy Notice