VOYAGE LEARNING CAMPUS

Voyage Learning Campus

DATA PROTECTION POLICY

This policy has been adopted by the Management Committee on:	
Date adopted:	26th November 2020
Signed:	
Next review due:	November 2022

Voyage Learning Campus (VLC)
Data Protection Policy

To be read in conjunction with the following documents:

- ***VLC Data Security Plan***

1.1 **The Voyage Learning Campus** collects, stores and processes personal information about staff, students, parents, Management Committee members, visitors and other individuals who come into contact with the school in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018) . The policy applies to all data, regardless of whether it is in paper or electronic format.

1.2 This information is gathered in order to enable it to provide education and other associated functions. In addition, there will be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations. The policy should be read in conjunction with the VLC Data Security Plan (May 2017).

1.3 Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. The VLC will renew this registration annually or as otherwise legally required. Schools also have a duty to issue a Privacy Notice to all students/parents; this summarises the information held on students, why it is held and the other parties to whom it may be passed on. A Data Collection Form is issued to all parents upon admission to the school highlighting the VLC Privacy Notice (appendix A) which is available on the VLC website.

2. Purpose

2.1 This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the GDPR and the Data Protection Act 2018, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

2.2 All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

3. Roles and Responsibilities

This policy applies to all staff employed by the VLC and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

3.1 **Management Committee**
The Management Committee has overall responsibility for ensuing that the VLC complies with all relevant data protection obligations.

3.2 **Data Protection Officer**

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description. Our DPO is I-West and is contactable via i-west@bathnes.gov.uk, Telephone number 01225 395959

3.3 **Principal**

The Principal acts as the representative of the data controller on a day-to-day basis.

3.4 **All staff**

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach or near-miss.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

3. What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

4. Data Protection Principles

4.1 The VLC will comply with the data protection principles of the GDPR specified in Article 5. These are that personal data must be

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

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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;
- 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;
- 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.
- Accountability principle – The School complies with its obligations under data protection laws including the GDPR and can demonstrate this via the measures set out in this policy, including:
    - Completing Data Protection Impact Assessments (DPIAs) where the School's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies. This largely involves special category personal data and CCTV. However, the School will liaise with the DPO who will advise on this process. Any activity involving the processing of personal data must be registered on the Register of Processing Activity and reviewed, at the very least, annually;
    - Integrating data protection into internal documents including this policy, any related policies and Privacy Notices;
    - Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; the School also maintains a record of attendance;
    - Regularly conducting reviews and audits to test its privacy measures and ensure compliance with relevant legislation and school policies;
    - Maintaining records of its processing activities for all personal data that it holds.

4.2 The VLC will adopt the appropriate technological and organisational measures to ensure compliance with the Data Protection Principles by carrying out the necessary procedures. The concept of data protection by design will be a guiding principle in achieving the security of individual's data protection rights.

4.3 A Data Protection Impact Assessment (DPIA) will be conducted prior to any high risk processing involving special categories of personal data or any extension to CCTV coverage at VLC.

4.4 In all aspects of our work we will ensure that the rights of the data subject are protected by all practicable measures associated with the conduct of our work. The rights of the data subject as defined in Chapter iii of the GDPR are;

a) The Right to be informed in a clear, concise and transparent manner
b) The Right of access
c) The Right to rectification
d) The Right to erasure
e) The Right to restrict processing
f) The Right to data portability
g) The Right to object
h) Rights related to automated decision making

5. General Statement

5.1 The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected – through Privacy Notices
- Inform individuals when their information is shared, and why and with whom it was shared – through Privacy Notices
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
    - The VLC keeps electronic data indefinitely and is held securely on corporate systems
    - The VLC destroys based legacy data in a controlled manner using industry specialists
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

6. Response time in the application of legislation

a) Subject Access Requests (SARs) whereby an individual may request information held by the VLC about themselves or a nominated individual on their behalf must be responded to within 1 month,

b) Where the above is found to be complex or numerous an extension may be granted allowing an additional 2 months however the subject must be informed within 1 month of their request,

c) No fee shall be charged for the above except where it is found to be excessive, repetitive or manifestly unfounded in accordance with article 12 of the GDPR,

Subject Access Requests (SARs) should be submitted in writing, either in a letter, email or fax to the Data Protection Officer. They should include the name of the individual, correspondence address, contact number and email address and details of the information required. A SAR can be made verbally but VLC will follow up with a request to document the details for its own records management practices. If staff receive a SAR they must immediately inform the Schools Operations Manager

6.1 An individual when making a SAR is entitled to the following.

- Confirmation that their data is being processed;
- Access to their personal data;
- Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

7. Data Retention

7.1 Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

7.2 Except where a specified retention period has been defined in accordance with the purpose of the activity any period of retention is defined by the Voyage Learning Campus record retention schedule a copy of which is available on request.

8. Complaints

8.1 Where an individual makes a complaint relating to the processing of their personal data or is unhappy with any response to an SAR, FOI or EIR (if appropriate) request they may request an internal review (IR) be conducted. Requests for an IR should be within 40 days of the original response. The responsibility for the conduct of an IR is with the Voyage Learning Campus who will discuss with the appointed DPO i-west. The VLC contact is the Schools Operations Manager.

8.2 If an individual is unhappy with the outcome of the IR they have the right to appeal to the Information Commissioner's Office (ICO) for assessment, the ICO is contactable at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

9. Personal Data Breaches

9.1 The VLC will make all reasonable endeavors to ensure that there are no personal data breaches.

9.2 For the purposes of this policy data breaches will include both suspected and confirmed incidents.

An incident can include, but is not limited to:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*
- Equipment failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data *(e.g. login details, emails to the wrong recipient, not using BCC, post to the wrong address)*
- Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire or flood
- Human error
- Breaches of policy such as
    - Server Room door left open
    - Filing cabinets left unlocked
    - Temporary loss / misplacement of confidential or sensitive data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*

Near misses can include, but are not limited to, scenarios such as emails sent to the wrong recipient where a non-delivery report bounces back.

9.3 Wherever it is believed that a security incident has occurred or a 'near miss' has occurred, the DPO will be informed immediately and the Security Incident Management (SIM) process will be carried out. The SIM is designed to manage, investigate, report and provide 'Learning from Experience' (LFE) to avoid future incidents occurring.

9.4 In any case an incident must be reported no later than 24hours from identification, except where a malicious incident has occurred. The learning culture within the VLC will seek the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes.

9.5 Where appropriate, we will report the data breach to the ICO within 72 hours.

10. Training

10.1 All staff and Management Committee members are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the VLC's processes make it necessary.

11. Monitoring and discipline

11.1 Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the VLC, in consultation with the Senior Leadership Team, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

12. Contacts

12.1 If you have any enquires in relation to this policy, please contact the school by letter or email to the School Operations Manager, Voyage Learning Campus, Oldmixon Crescent, Ashcroft House, Weston super Mare, BS24 9AX who will also act as the contact point for any subject access requests.

12.2 Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745