Data Protection / Handling Policy

Context and overview

Introduction

Vibrance Education collects, stores and professes personal information about staff, students, parents or carers and other individuals who come into contact with the provision of the General Data Protection Regulation (GDPR) and the expected requirements of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

This information is gathered to enable the provision of education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the provision complies with its statutory obligations.

This policy describes how personal data must be collected, handled, and stored to meet the company's data protection standards and comply with the law.

Why this policy exists

This data protection policy ensures Vibrance Education:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 2018 describes how organisations—including Vibrance Education—must collect, handle, and store personal information. It also meets the requirements of the Protection of Freedoms Act 2012 regarding our use of data.

These rules apply regardless of whether data is stored electronically, on paper or other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

Eight important principles underpin the Data Protection Act. These say that personal data must:

1. Be processed fairly and lawfully
2. Specific for its purpose
3. Be adequate and only for what is needed
4. Be accurate and kept up to date
5. Not kept longer than needed
6. Consider people's rights
7. Kept safe and secure
8. Not be transferred outside the EEA

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for using surveillance cameras and personal information.

Data Protection / Handling Policy

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject- students and families	The identified or identifiable individual whose personal data is held or processed.
Data controller- management	A person or organisation that determines the purposes and the means of processing personal data.
Data processor / 3rd party - ClassDojo, 365, Portland, SIM's, Site builder, WIX, google drive and pension provider.	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Data Protection / Handling Policy

People, risks and responsibilities

Policy scope
This policy applies to:

- The admin of Vibrance Education
- All branches of Vibrance Education
- All staff and volunteers of Vibrance Education
- All contractors, suppliers and other people working on behalf of Vibrance Education

It applies to all company data relating to identifiable individuals, even if that information technically falls outside the Data Protection Act 2018. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- plus any other information relating to individuals

Data protection risks
This policy helps to protect Vibrance Education from some genuine data security risks, including:

- **Breaches of confidentiality.** For instance, information is being given out inappropriately.
- **Need to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully accessed sensitive data.

Responsibilities
Everyone who works for or with Vibrance Education has some responsibility for ensuring data is collected, stored and handled appropriately.
Each team handling personal data must ensure that it is handled and processed in accordance with this policy and data protection principles.
However, these people have key areas of responsibility:

The **board of directors** is ultimately responsible for ensuring Vibrance Education meets its legal obligations.

The **management** is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Review all data protection procedures and related policies per an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.

- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with individual requests to see Vibrance Education's data about them (called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

The **IT manager** is responsible for:

- Ensuring all systems, services and equipment storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software are functioning correctly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

The **staff** are responsible for:

- Collecting, storing and processing any personal data by this policy
- Informing the provision of any changes to their data, such as a change of address
- Contacting the managers in the following circumstances:
  - If you have any questions about the operation of this policy, data protection law, retaining personal data, or keeping personal data secure,
  - If they have any concerns about this policy not being followed,
  - If they are still determining whether 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 UK.
  - If there has been a data breach.
  - Whenever they engage in a new activity, it may affect the privacy rights of individuals.
  - If they need help with contracts or sharing personal data with third parties.

Third-Party Data Processors

Where external companies are used to process personal data on behalf of Vibrance Education, responsibility for the security and appropriate use remains with Vibrance Education.

Where a third-party data processor is used:

- A data processor must be chosen that provides sufficient guarantees about its security measures to protect the processing of personal data.
- Reasonable steps must be taken so that such security measures are in place.
- A written contract establishing what personal data will be processed and for what purpose must be set out.
- A data processing agreement, available from the Governance Team, must be signed by both parties.

Students are responsible for:

- familiarising themselves with the Data Protection Agreement
- ensuring that the personal data provided to Vibrance Education is accurate and current.

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should be kept private**. When access to confidential information is required, employees can request it from their line managers.
- **Vibrance Education will train** all employees to help them understand their data-handling responsibilities.
- Employees should keep all data secure by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and should never be shared.
- Personal data **should not be disclosed** to unauthorised people within the company or externally.
- Data should be **regularly reviewed and updated** if necessary. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the management if they need clarification on any aspect of data protection.

Data storage

We will only collect personal data for specified explicit and legitimate reasons. When we first collect their data, we will explain these reasons to the individuals.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where necessary to do their jobs.

When staff no longer need their personal data, they must ensure it is deleted or anonymised. This will be done according to the provision's record retention schedule, which can be found on the website.
These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.
Data **stored on paper** should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- The paper or files should be kept **in a locked drawer or filing cabinet when not required**.
- Employees should ensure paper and printouts are kept out of the reach of unauthorised people, such as on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer

required.

- When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be locked securely when not being used.
- Data should only be stored on **designated drives and servers** and uploaded to an **approved cloud computing service**.
- Servers containing personal data should be **stored securely**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, per the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices, such as tablets or smartphones, without encryption.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

Personal data is of value to Vibrance Education if the business can use it. However, it is when personal data is accessed and used that it can be at the most significant risk of loss, corruption or theft:

- When working with personal data, employees should ensure **that their computers' screens are always locked** when left unattended.
- Personal data **should not be shared informally**. It should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should **not be transferred outside of the UK without permission.**
- Employees **should not save copies of personal data to their computers**
- **Always access and update the central copy of any data.**

Data Accuracy

The law requires Vibrance Education to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Vibrance Education should put into ensuring its accuracy.

All employees who work with data are responsible for taking reasonable steps to ensure it is kept as accurate and up-to-date as possible.

- Data will be held in **as few places as necessary**, and staff should not create unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated, such as** confirming a detail when they call.
- Vibrance Education will make it **easy for data subjects to update the information** Vibrance Education holds about them.
- Data should be **updated as inaccuracies are discovered**. For instance, if a family can no longer be reached on their stored telephone number, it should

be removed from the database.

- **The manager checks databases against industry suppression files** every six months.

Sharing Personal Data

We will not usually share personal data with anyone who is not linked to a student, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data-sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- For research and statistical purposes, if personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them respond to an emergency affecting any of our pupils or staff.

When we transfer personal data to a country, we will do so by data protection law.

Subject access requests

All individuals and parents who are the subject of personal data held by Vibrance Education are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed on **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be emailed and addressed to the manager at enquiries@vibrance-education.co.uk. The manager can supply a standard request form, although individuals do not have to use this.

The manager will always verify the identity of anyone making a subject access request before handing over any information.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge
- We may tell the individual we will comply within three months of receipt of the request, where the request is complex or numerous. We will inform the individual of this within one month and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee that considers administrative costs.

A request will be deemed unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above) and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict the processing of their data or object to the processing of it (in certain circumstances)
- Prevent the use of their data for direct marketing
- Challenge processing, which has been justified based on public interest
- Please request a copy of the agreements under which their data is transferred outside of the UK
- Object to decisions based solely on automated decision-making or profiling (decisions taken with no human involvement that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the management. If staff receive such a request, they must immediately forward it to the management.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the data subject's consent.
Under these circumstances, Vibrance Education will disclose the requested data. However, the manager will ensure the request is legitimate, seeking assistance from the board and the company's legal advisers where necessary.

Providing information

Vibrance Education aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement that sets out how it uses data relating to individuals.
[This is available on request. A version of this statement is also available on the company's website.]

Technology

CCTV

We use CCTV in various locations around the provision site to ensure its safety. We will adhere to the ICO's code of practice for using CCTV.

We do not need to ask individuals' permission to use CCTV, but we clarify where individuals are being recorded. Security cameras are visible and accompanied by prominent signs explaining that CCTV is in use.
Any enquiries about the CCTV system should be directed to the head of provision.

Photographs and videos

As part of our provision activities, we may take photographs and record images of individuals within our provision.

We will obtain written consent from parents/carers or pupils aged 18 and over for photographs and videos of pupils to be used for communication, marketing, and promotional materials.

When we need parental consent, we will clearly explain how the photograph and video will be used by both the parent/carer and pupil. When we don't need parental consent, we will clearly explain how the pupil will use the picture and video.

Uses may include:

- Within provision on notice boards and in provision magazines, brochures, newsletters, etc.
- Outside of provision by external agencies such as the provision photographer, newspapers, campaigns
- Online on our provision website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will

delete the photograph or video and not distribute it further.

When using photographs and videos this way, we will not accompany them with any other personal information about the child to ensure they cannot be identified.

See our child protection and safeguarding policy for more information on our use of photographs and videos.

Data protection by design and default

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

- Appointing a suitably qualified staff and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing privacy impact assessments where the provision's processing of personal data presents a high risk to the rights and freedoms of individuals and when introducing new technologies (the management will advise on this process)
- 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; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our provision and management and all information we are required to share about how we use and process their data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, the data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

Disposal of data

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

For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to dispose of records safely on the provision's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

What Vibrance Education will do if GDPR is breached?

Breaches

All staff members must report data protection breaches or contact the management if they have concerns about such a breach (office@Vibrance Education.com). This will allow the appropriate personnel to investigate further and take the proper steps to fix the issue promptly.

What to do if staff fail to comply?

If data protection is not followed, this will be discussed in supervision meetings with staff and may involve staff warnings.

Staff training

Staff will have regular updates and training in GDPR.

Reviewing:

If necessary, this guide and policy will be reviewed and updated every two years. The Freedom of Information publication scheme will also be reviewed regularly. Staff will check that if they add a new piece of recorded information to the provision's portfolio, this is covered within the scheme.

Appendix 1:

Requests for information

- The Freedom of Information Act came into force on 1st January 2005. Under this Act, all provisions that receive a written or emailed request for information which they hold or publish are required to respond within 20 working days
- The provision will provide information on where to access the information required, e.g., the website link or details of a charge if the publication/ information is charged or sent any free information. If the item is charged, the provision must only be provided once the payment is received.
- A refusal of any requested information must state the relevant exemption that has been applied or that the provision does not hold the information and explain what public interest test has been made if this applies.
- If another organisation publishes the information, the provision can direct the enquirer to the organisation that supplied the information or publication unless it is legal and possible to provide it directly.
- It will not be legal to photocopy a publication and supply this to an enquirer unless the provision owns the copyright.
- The provision will keep the original request and note against this who dealt with the request and when the information was provided
- Any complaint about the provision of information will be handled by the Head of Provision or a delegated member of the Senior Leadership Team. All complaints should be in writing and documented.
- All enquirers should be advised that they may complain to the Information Commissioner if they are unhappy with how their request has been handled.

[Your full address]
[Phone number]

[The date]

Vibrance Education

Dear Sir or Madam

Subject access request

[Your full name, address, and other details to help identify you and the information you want.]

Please supply the information about me I am entitled to under the GDPR relating to: [give specific details of the information you want], for example

- your personnel file.
- Emails between 'A' and 'B' (between 1/6/11 and 1/9/11).
- Your medical records (between 2006 & 2009) were held by Dr 'C' at 'D' hospital.
- CCTV camera situated at ('E' location) on 23/5/12 between 11am and 5pm.

If you need any more information or a fee, please let me know as soon as possible.

It may be helpful for you to know that a request for information under the GDPR should be responded to within 40 days.

Please pass this letter on to your Data Protection Officer if you do not usually handle these requests. If you need advice on dealing with this request, the Information Commissioner's Office can assist you and can be contacted on 0303 123 1113 or at ico.org.uk

Yours faithfully

[Signature]