

Venture Learning

Data Protection Policy &

General Data Protection Regulations

Venture Learning

Document Owner	Rhys Griffiths
Version	1.0
Effective From	21/01/2019
Next Review Date	21/01/2020

Introduction

Venture Learning is committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of data about the young people who access our provision, their parents/carers and third party services. All personal information will be collected and dealt with appropriately to ensure that each stakeholder's rights are upheld at all times.

The Data Protection Act 1998 (DPA) governs the use of information about people (personal data). Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs. Venture Learning is responsible for deciding what data will be held, as well as how it will be held and used.

All staff and volunteers will be personally responsible for processing and using personal information in accordance with the Data Protection Act. Those who have access to personal information will be expected to read and comply with this policy.

Under the data protection act 1998, companies and charities have a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

- unauthorised or unlawful processing of personal data;
- unauthorised disclosure of personal data; and,
- accidental loss of personal data.

Personal data relates to data of living individuals who can be identified from that data and use of that data could cause an individual damage or distress. This does not mean that mentioning someone's name in a document comprises personal data; however, combining various data elements such as a person's name and salary or religious beliefs etc. would be classed as personal data, and falls within the scope of the Data Protection Act.

Venture Learning collects a large amount of personal data every year including but not limited to: student records, parent/carer details, staff records, names and addresses of those requesting prospectuses, examination marks and references. In addition, we may be required to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

The purpose of this policy is to set out Venture Learning's commitment and procedures for protecting personal data. Venture Learning regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal with.

Key Staff and Contacts

Provision Based Contacts

Name	Role
Rhys Griffiths	**Head of Provision**
Holly Crann	**Deputy Head of Provision**
Contact details:	**Venture Learning** **19A Forester Street** **Netherfield** **Nottingham** **NG4 2LJ**
	www.venturelearning.co.uk
	0115 987 6621 / 07587 408 996
	Rhys.griffiths@venturelearning.co.uk
	Holly.crann@venturelearning.co.uk

The Supervisory Authority in the UK

Please follow this link to the ICO's website (https://ico.org.uk/) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.

Section 1: Principles

Article 5 of the GDPR requires that personal data shall 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; and,
- 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.

Venture Learning will need to collect data for specific purposes. In such circumstances, we will let people know why we are collecting their data and it is our responsibility to ensure the data is only used for this purpose.

Individuals have a right to have data corrected if it is wrong, to prevent use which is causing them damage or distress, or to stop marketing information being sent to them.

Section 2: Operational Procedures

2.1 Lawful Basis for processing personal information

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

- processing is necessary for the performance of a task carried out in the public interest;
- processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the data controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party; or,
- the data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent.

2.2 Sensitive Personal Information

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- there is a lawful basis for doing so; and,
- one of the special conditions for processing sensitive personal information applies:
    - the individual (data subject) has given explicit consent;
    - the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject;
    - the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
    - the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim;

- the processing relates to personal data which are manifestly made public by the data subject;
- the processing is necessary for the establishment, exercise or defence of legal claims;
- the processing is necessary for reasons of substantial public interest;
- the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services; or,
- the processing is necessary for reasons of public interest in the area of public health.

Venture Learning's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Unless Venture Learning can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that we can demonstrate compliance with the GDPR.

2.3 Data Protection Impact Assessments (DPIA)

All data controllers are required to implement 'Privacy by Design' when processing personal data. This means Venture Learning's processes must embed privacy considerations and incorporate appropriate technical and organisational measures in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and,
- what measures can be put in place to address those risks and protect personal information.

The DPIA template can be obtained from the Data Protection Toolkit by the Department for Education.

2.4 Documentation and records

Written records of processing activities must be kept and recorded including:

- the name(s) and details of individuals or roles that carry out the processing;
- the purposes of the processing;
- a description of the categories of individuals and categories of personal data;
- categories of recipients of personal data;
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;
- retention schedules;
- a description of technical and organisational security measures;
- information required for privacy notices;
- records of consent;

- the location of personal information;
- DPIAs; and,
- records of data breaches.

Records of processing of sensitive information are kept on:

- the relevant purposes for which the processing takes place, including why it is necessary for that purpose;
- the lawful basis for our processing; and,
- whether the personal information is retained or erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

Venture Learning should conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

- carrying out information audits to find out what personal information is held;
- talking to staff about their processing activities; and,
- reviewing policies, procedures, contracts and agreements to address retention, security and data sharing.

2.5 Privacy Notices

Venture Learning will issue privacy notices as required, informing data subjects (or their parents, depending on age of the student, if about pupil information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the data protection officer, how and why the School will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from an external service or commissionaing school) Venture Learning must check that the data was collected by the third party in accordance with the GDPR and on a basis which is consistent with the proposed processing of the personal data.

Venture Learning will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Venture Learning will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes.

2.6 Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

2.7 Data Minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

Venture Learning will maintain a retention schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the schedule. This includes requiring third parties to delete such data where applicable.

2.8 Individual Rights

Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- to be informed about how, why and on what basis that information is processed;
- to obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request;
- to have data corrected if it is inaccurate or incomplete;
- to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten');
- to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where Venture Learning no longer need the personal information, but you require the data to establish, exercise or defend a legal claim;
- to restrict the processing of personal information temporarily where you do not think it is accurate, or where you have objected to the processing;
- in limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format;
- to withdraw consent to processing at any time (if applicable);
- to request a copy of an agreement under which personal data is transferred outside of the EEA;
- to object to decisions based solely on automated processing, including profiling;
- to be notified of a data breach which is likely to result in high risk to their rights and obligations; and,
- to make a complaint to the ICO or a Court.

2.9 Information Security

Venture Learning will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow Venture Learning's acceptable usage policy.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users can access the personal data when they need it for authorised purposes.

All staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards Venture Learning has implemented and maintains in accordance with the GDPR and DPA.

2.10 Storage and Retention of Personal Information

Personal data will be kept securely in accordance with the Venture Learning's data protection obligations.

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. Personal information that is no longer required will be deleted in accordance with Venture Learning's Record Retention Schedule.

2.11 Data Breaches

A data breach may take many different forms:

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware or software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; or,
- blagging offences where information is obtained by deceiving the organisation which holds it,

Venture Learning must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. Venture Learning must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform the Head of Provision immediately that a data breach is discovered and make all reasonable efforts to recover the information.

2.12 Consequences of a Failure to Comply

Venture Learning takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and Venture Learning and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under Venture Learning's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

Section 2: Roles and Responsibilities

Venture Learning is the Data Controller under the DPA, and is legally responsible for complying with the Act, which means that it determines what purposes personal information held will be used for.

2.1 Head of Provision

The Head of Provision will act as the Data Protection Officer will be responsible for ensuring that this policy is implemented and will have overall responsibility for:

- ensuring that everyone processing personal information understands that they are contractually responsible for following good data protection practice;
- ensuring that everyone processing personal information is appropriately trained to do so;
- dealing promptly and courteously with any enquiries about handling personal information;
- describing clearly how Venture Learning handles personal information;
- regularly reviewing and auditing the ways Venture Learning holds, manages and uses personal information; and,
- regularly assessing and evaluating Venture Learning's methods and performance in relation to handling personal information.

2.2 All Staff

All staff should be familiar with this policy and adhere to the guidance and procedures laid out herein.

All staff must ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper or in a computer or recorded by some other means.

All staff and volunteers should be aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

During their employment, staff may have access to the personal information of other members of staff, students and third parties. Venture Learning expects staff to help meet its data protection obligations to those individuals. Staff with access to personal information must:

- only access the personal information that they have authority to access and only for authorised purposes;
- only allow other staff to access personal information if they have appropriate authorisation;
- only allow individuals who are not staff to access personal information if they have specific authority to do so;
- keep personal information secure (by complying with rules on access to premises, computer access, password protection, secure file storage and destruction etc.);
- not remove personal information, or devices containing personal information from the school's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection); and,
- not store personal information on local drives or on personal devices that are used for work purposes.