GENERAL DATA PROTECTION REGULATION (GDPR) POLICY
THE SEA VIEW TRUST (VALLEY COLLEGE)

INTRODUCTION

The Sea View Trust is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA).

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

Valley College is part of The Sea View Trust – a multi-academy trust incorporating a number of different schools and academies. When we refer to "we", "us", "our" or "the college" within this policy, we are referring to Valley College which is part of The Sea View Trust. The Sea View Trust is the 'data controller' for the purposes of data protection law.

Changes to data protection legislation shall be monitored and implemented in order to remain compliant with all requirements.

The legal bases for processing data are as follows:
1. **Contract**: the processing is necessary for the member of staff's employment contract or student placement contract.
2. **Legal obligation**: the processing is necessary for the college to comply with the law (not including contractual obligations)

The members of staff responsible for data protection are mainly

- Data Controller – The Sea View Trust (Trustees, Governors, Executive Principal, Head of College and its employees)
- Data Protection Officer (DPO)

All staff must treat all learner information in a confidential manner and follow the guidelines as set out in this document.

The college is also committed to ensuring that Trust staff are aware of data protection policies, legal requirements and that adequate training is provided to them.

The requirements of this policy are mandatory for all staff employed by the college and any third party contracted to provide services within the college.

Notification:

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller.

Details are available from the ICO:
https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO. If any member of staff becomes aware of any actual or suspected personal data breach, they should report it immediately to the Data Protection Officer in accordance with the Trust's Data Breach Procedure.

Personal and Special Category Data:
All data within the college's control shall be identified as personal, sensitive (special category) or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and special category data shall be as those published by the ICO for guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

The principles of the Data Protection Act shall be applied to all data processed:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- ensure that data is secure.

Fair Processing / Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, advocates and learners prior to the processing of individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-noticestransparency-and-control/

There may be circumstances where the college is required either by law or in the best interests of our learners or staff to pass information onto external authorities, for example local authorities, Ofsted, or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect. The intention to share data relating to individuals to an organisation outside of our college shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information. Any proposed change to the processing of individual's data shall first be notified to them. Under no circumstances will the college disclose information or data:

- that would cause serious harm to the learner or anyone else's physical or mental health or condition;
- indicating that the learner is or has been subject to abuse or may be at risk of it, where the disclosure would not be in the best interests of the learner;
- recorded by the learner in an examination;
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the college, the Trust or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed;
- in the form of a reference given to another college or any other place of education and training, the learner's potential employer, or any national body concerned with student admissions.

Data Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/integrity-and-confidentiality-security/

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

Data Access Requests (Subject Access Requests):

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to the Data Protection Officer. If any other member of staff receives a subject access request, the request should be forwarded to the Data Protection Officer without undue delay.

No charge will be applied to process the request.

Personal data about learners will not be disclosed to third parties without their consent, or the consent of their advocate (depending on the particular circumstances), unless it is obliged by law or in the best interest of the learner. Data may be disclosed to the following third parties without consent:

- **Other educational providers**

If a learner transfers from The Sea View Trust, their academic records and other data that relates to their health and welfare.

- **Examination authorities**

This may be for registration purposes, to allow the learners at our college to sit examinations set by external exam bodies.

• **Health authorities**
As obliged under health legislation, the college may pass on information regarding the health of learners in the college to monitor and avoid the spread of contagious diseases in the interest of public health.

• **Police and courts**
If a situation arises where a criminal investigation is being carried out, we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

• **Social workers and support agencies**
In order to protect or maintain the welfare of our learners, and in cases of suspected abuse, it may be necessary to pass personal data on to social workers or support agencies.

• **Educational division**
Colleges may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

Right to be Forgotten:

Where personal data is no longer required for its original purpose, an individual can request that the processing is stopped and all their personal data is erased by the college including any data held by contracted processors. This right only applies in particular circumstances and there are a number of circumstances in which it would not apply. Any request to exercise the right to be forgotten or erasure should be forwarded to the Data Protection Officer without undue delay.

Photographs and Video:

Images of staff and learners may be captured at appropriate times and as part of educational activities for use in college only.

Unless prior consent from advocates/earners/staff has been given, the college shall not utilise such images for publication or communication to external sources.

It is the college's policy that external parties (including advocates) may not capture images of learners or pupils during such activities without prior consent.

Location of information and data:

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the college day.

Sensitive or special category data should not be removed from the college site, however the college acknowledges that some staff may need to transport data between the college and their home in order to access it for work in the evenings and at weekends.

This may also apply in cases where staff have offsite meetings, or are on college visits with learners.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the college site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the college site, the information should not be on view in public places, or left unattended under any circumstances.

- Unwanted paper copies of data, sensitive information or learner files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or learner by name.

- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.

- If it is necessary to transport data away from the college, it should be downloaded onto an encrypted USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only.

- USB sticks that staff use must be password protected. These guidelines are clearly communicated to all college staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Disposal:

The college recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance:

https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf

The college has identified a qualified source for disposal of IT assets and collections. The college also uses our own shredder to dispose of sensitive data that is no longer required.

This Policy will be reviewed by the Board of Trustees on a bi-annual cycle

Person responsible for the Policy:	College Business Lead (Valley College)
Colleagues affected by this Policy:	All Trust employees and stakeholders
Approved and adopted by Trustees:	May 2018
Reviewed by DPO	September 2020
Next Review:	2022