General Data Protection Regulations (GDPR) in

Forth Valley College

1. What is GDPR?

GDPR is the legislation which governs what personal information (see section 3 below for definitions) an organisation can keep along with how it can use, retain and pass on personal information.

GDPR was created to address the changes in society which result in far more personal data being available about individuals. It strengthens the rights of individuals to have more control over their data (subject to specific exemptions) and enables them to see, amend and, where appropriate, have their data deleted.

2. GDPR Principles

The College must ensure any personal data it holds or utilises must be –

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

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 they are processed;

d) 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;

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 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

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.

The College must be in a position to **demonstrate** that it complies with these principles and these should be borne in mind when any existing or new College system which contains personal data is updated/developed.

3. What is Personal Data and Sensitive Personal Data

GDPR only covers data the College holds which is either personal data or sensitive personal data.

The definitions of these are as follows –

Personal Data – any information relating to an identified or identifiable natural person ("data subject"); an identifiable 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, online

identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Sensitive Personal Data - are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

4. Security of Data

Data covered by GDPR can be stored both as electronic and hard copy data. The College has a number of processes in place to ensure the security of this data to which all staff much comply.

Physical Access to Data

All areas where data is stored (primarily workrooms/offices etc) must always be locked when there are no staff members present.

Printouts/application forms etc containing personal data must not be left out in plain sight on desks.

Storage cabinets/cupboards/desk drawers must always be locked overnight or when a staff area is unattended.

Digital Access

The College has an I.T. Security Policy in place which governs IT equipment within the College and all staff should familiarise themselves with this Policy.

Additionally staff are specifically prohibited from –

- Disclosing their password
- Downloading/saving personal data onto memory sticks or other removable media
- Sending personal data to their own personal email/social media account
- Sharing personal data from College systems on social media
- Forwarding to/or storing personal data on any online system (commonly referred to as a Cloud service) which has not been approved by the College – should staff members wish to utilise a new cloud service, approval must be obtained from the Vice Principal Information Systems and Communication

Staffing and Contractors

All staff members are required to undergo a PVG check as part of their contract of employment with the College. The HR team should pay close attention to PVG returns in terms of data related issues in an applicant's history.

Staff should be aware when contractors are carrying out works within their area and ensure that no personal data is left in plain sight.

Contractors who require access to College systems should only be provided with the minimum level of access to enable them to carry out their duties.

5. Data Protection Officer (DPO)

The GDPR legislation requires that the College have a designated DPO in place. The DPO has a range out duties outlined in the legislation, including ensuring all staff are adequately trained in GDPR and their responsibilities. A DPO may not be dismissed as a result of performing their duties.

To ensure transparency and good governance, the DPO also has the right to raise any concerns they may have directly with the Board of Management of the College.

6. Training

The College will ensure all staff are trained in GDPR. This mandatory training will be refreshed on a bi-annual basis and also forms part of all induction courses for new employees.