System/Data Special Access Request Policy

POLICY STATEMENT:

During the normal daily processes, there are occasions where a member of staff or a student will need access to information or systems not usually covered by the access given by default to their account based on their role and location. This policy is designed to ensure access is only granted where needed and removed once no longer required.

POLICY DETAIL:

Requests for additional access will usually come through to either the People Services Department or Digital Department. These requests will usually be for access to (but not limited by) door, network, cloud, SharePoint and other internal or external systems. When these requests come through the following steps will be followed.

- The request for access will be clarified to fully understand what is required and why, this will ensure that only the correct access will be given. This will include finding out how long the access is needed and if this access is only to the data or to be able to make changes/create new data.
- Authorisation to access this data is needed, this can be completed by,
  - Assessing the user job title and comparing the access requested with another employee in the same role/department.
  - Contacting the manager, either of the employee or the owner of the data or systems.
  - Discussion with the People Services Department
- Requests for special access must go through the relevant helpdesk systems and be properly documented, including what access has been given, what was done to ensure authorisation has been given and how long access is needed.
- If access is time-limited, then the ticket in the relevant helpdesk system is to be kept open until it has been agreed the access can be removed. Once that date is reached then access will be removed unless further instruction given and documented.

Failure to follow this process could mean access to data is given to unauthorised users and be in breach of our commitment to keep data secure. Any data breach needs to be considered under the GDPR regulations and, where necessary, reported to the Information Commissioners Office in accordance with the group data breach procedure.

When a new role is created or staff member changes role, it is the line manager's responsibility to ensure appropriate access is provisioned to the role and any permissions no longer needed are removed. For example, if a member of staff previously helped with People Services data entry and now works with Student data entry, all access to the People Services system should be revoked.

In the case of access to highly sensitive information this must come from the College Principal or Senior Manager e.g. access to budget packs and pay information.

Regular Review

With most files now stored in Teams, access is now the responsibly of the team owners. Access to these teams should be reviewed at least annually and specifically after any organisation changes.
Centrally managed systems will be checked at least annually, however in practice most will be checked more frequently when additions are made. Privileged access accounts must be confirmed every 3 months with the director or suitable senior manager.

Owner: Group Director of Digital
Approving Body: GLB
Stage of approval: Approved
Date of approval: June 2023
Page 1 of 1