CHURCHILL COLLEGE
CAMBRIDGE CB3 0DS

Data Security Policy

Policy Name	Data Security
Purpose	The purpose of this policy is to set out the data security measures taken by the College and the responsibilities of employees, with regard to these measures.
Owner	Head of IT
Contact	Head of IT (David Spaxman)
Approved By	College Council
Approval Date	8 October 2024
Next Review Due	MT2027
Version and Recent Changes	Previously within Staff Handbook. V1 of the policy as an independent document MT24.

1. Introduction

1.1. The purpose of this policy is to set out the data security measures taken by the College and the responsibilities of employees, with regard to these measures.

2. Scope

2.1. This policy applies to all users of College IT Systems, or those who utilise College data digitally, even if they have not been specifically given their own personal account to use.

3. Responsibilities

3.1. Overall responsibility for data security lies with College Council. The ICT committee, which reports to College Council, has oversight of matters relating to IT systems and the security of data held on these systems will be reviewed by the committee on an annual basis. Operational responsibility lies with the Bursar, through the Head of I.T.

3.2. Heads of Department are responsible for ensuring that employees are given appropriate permissions to access College files and applications and for ensuring their staff are aware of this policy.

3.3. Employees are responsible for acting in accordance with this policy and related procedures, as listed below.

4. Access to Secure IT Areas

4.1. Only employees who are appropriately trained, or otherwise require access owing to the College Health, Safety and Fire policies are permitted permanent access to these areas. Permission to access these areas may be given by the Head of I.T. or the Bursar. Further details on how employees may gain access to these areas, and how they should conduct themselves within these areas, are given in the Access to Secure IT Areas Procedure.

5. Local Working

5.1. Employees, workers and temporary contractors, who work locally within the College, and require or already have user accounts on the College's IT services should abide by the provisions of the Local Working Procedure.

6. Application Access

6.1. Employees who have been given access to the College's IT services and require access to restricted application packages are required to adhere to the College's Application Access Procedure.

7. Remote Working and Use of Own Devices

7.1. Employees who work remotely, for example from home, must adhere to the College's Remote Working and Use of Own Device Procedures. Please be aware that at present there is not an active policy nor support from the College for using personally owned devices to work.

8. Remote Email Access

8.1. Employees must adhere to the College's Mobile Email Access Procedure in conjunction with the College's Policy on IT Facilities, The Internet and Electronic Mail.

9. Hard Copy Data

9.1. When personal data or confidential data is stored on paper, it 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.

9.2. When not required, the paper or files should be kept in a locked drawer or filing cabinet. Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer. Data printouts should be shredded and disposed of securely when no longer required.

10. Breach of Policy Reporting/Results

10.1. If an employee is found to not comply with this policy disciplinary action may be taken, up to and including dismissal for gross misconduct.

11. Appendices

i. Access to Secure IT Areas Procedure
ii. Local Working Procedure
iii. Application Access Procedure
iv. Remote Working and Use of Own Device Procedures
v. Mobile Email Access Procedure

12. Other related documents

i. IT Facilities, The Internet and Electronic Mail Policy