Exeter College Data Protection Policy – Summary

This document is meant to be an easier to read summary of the full College Data Protection document accessible from the college website.

1. Purpose & Scope

This policy formalizes Exeter College's approach to information security, ensuring compliance with:

- UK GDPR (General Data Protection Regulation)
- Data Protection Act 1998
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- Human Rights Act 1998
- Counter-Terrorism and Security Act 2015 (PREVENT duty)

It applies to all staff, students, visitors, and external contractors who handle or process college data, covering:

- Personal and sensitive information (e.g., student and staff records)
- Research data
- Financial and operational data
- IT systems and networks

The policy is reviewed annually by the Governing Body to ensure continued relevance.

---

2. Core Data Protection Principles

The college must protect Confidentiality, Integrity, and Availability (CIA) of all data:

- Confidentiality: Ensuring only authorized individuals can access personal or sensitive data.
- Integrity: Preventing unauthorized alterations or corruption of data.
- Availability: Making sure authorized users can access necessary data when required.

Key legal obligations under UK GDPR:

- Lawful Processing: Data can only be processed for a clear, legal purpose.
- Data Minimization: Collect only what is necessary.
- Security Measures: Implement appropriate safeguards to prevent unauthorized access, leaks, or breaches.
- Breach Reporting: Notify the Information Commissioner's Office (ICO) within 72 hours if a personal data breach occurs.

---

3. Information Security Measures

All college members handling data must adhere to the following security

practices: Physical Security

- Apply a clean desk policy - lock sensitive paper records and USB drives in secure storage.
- Dispose of confidential waste using shredding or approved disposal methods.
- Use identity verification before granting access to physical documents.

Digital Security as normal every day practice

- Encryption:
  - Sensitive data stored on portable devices (USBs, laptops, smartphones) must be encrypted.
- Device Protection: All networked devices must be:
  - Password-protected
  - Running up-to-date anti-virus, firewall, and security patches
- Secure File Transfers:
  - Personal data should not be stored on public cloud services (e.g., Dropbox, WeTransfer) unless properly risk assessed.
- Email Precautions:
  - Avoid mass email leaks (e.g., using BCC instead of CC).
- Remote Access:
  - Work from outside the college must use secure VPN connections.

4. Data Classification & Risk Assessment

Personal Data:

- Any information that can identify an individual (e.g., names, emails,

student records). Special Category Data (Higher Protection Required):

- Race, ethnicity, politics, religion, trade union membership
- Health, biometric data, sexual orientation
- Criminal records or allegations

Risk Assessment:

- Each department must assess the sensitivity of its data and apply the appropriate security measures.

Access Control:

- Data access is granted on a need-to-know basis, reviewed annually.

5. Data Breach & Incident Reporting

A personal data breach is any unauthorized:

- Access (e.g., hacking, lost laptop)
- Disclosure (e.g., sending an email to the wrong person)
- Alteration or loss (e.g., accidental deletion)

Breach Response Protocol

1. Immediate Reporting:
   - All breaches must be reported within 72 hours to DataProtection@exeter.ox.ac.uk.
   - Notify your line manager or Rector.
   - Do not attempt to investigate independently.
2. Investigation & Notification:
   - The Data Protection Officer (DPO) determines if the breach must be reported to the ICO and affected individuals.

- The college documents all breaches, their impact, and remediation steps.

3. Consequences of Non-Compliance:
    - Failure to report a breach can lead to severe fines and disciplinary action.

6. IT & Network Security Policies

System Access & Passwords

User Authentication:

- Strong passwords (15+ characters, mix of letters/numbers/symbols)
- Multi-Factor Authentication (MFA) where applicable

Access Restrictions:

- Users should only have the minimum privileges necessary for their role.
- Shared computers require user authentication.

Network Security

- College firewalls and intrusion detection systems protect against cyber threats.
- The IT team logs unauthorized access attempts, port scans, and denial-of-service attacks.
- Logs are kept for at least 60 days to track security events.

Use of Personal Devices (BYOD) - If accessing college systems from a personal device, the user must ensure:

- Up-to-date security software is installed.
- College data is encrypted before storage.
- Personal cloud storage is not used for sensitive information.

7. Acceptable Use & Monitoring

Email & Internet:

- Only work-related use is allowed; personal or commercial use is prohibited.
- All email is monitored for security threats (spam, malware).
- Mass emails must follow strict college guidelines.

Monitoring & Compliance:

- The college reserves the right to monitor IT use.
- Any unauthorized or illegal activity (e.g., accessing extremist content under PREVENT) will be investigated.
- Violations may result in access revocation or disciplinary action.

8. Data Retention & Disposal

Retention Periods:

- Data should be kept only as long as necessary.
- Personal data that is no longer needed should be securely deleted.

Computer Equipment Disposal:

- Before disposal, all storage devices must be securely wiped or physically destroyed.
- Computers may be repurposed or donated if all data has been removed.

9. Employee Responsibilities & Training

- All college staff must complete annual data protection training.
- Employees must read and acknowledge this policy before handling data.
- Failure to comply with security procedures may result in disciplinary action.

Final Notes

This policy is a legally binding document for all Exeter College members. The Governing Body, IT team, and Data Protection Officer ensure ongoing compliance. Regular risk assessments, audits, and training help maintain high security standards.

By College Order 25/028, this policy was approved by Governing Body on 12th March 2025 with immediate effect, and is to be reviewed by the 31st March 2026, and was also approved for display on the website.