DATA PROTECTION POLICY

Role Responsible:	Vice Principal (Community Engagement & Business Development)
Written by:	DPO / Vice Principal (Community Engagement & Business Development)
Date Approved:	19/4/2026
Approved by:	Senior Leadership Team
Publication	Google Shared Drive – Itchen Staff – Staff Policies & Website
Review cycle:	Biennial (every 2 years)
Next Review Date:	01/05/2028

DATA PROTECTION POLICY

Contents

1. PURPOSE

Itchen Sixth Form College ("the College") is committed to protecting the rights and freedoms of individuals in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This policy sets out how the College collects, processes, stores and protects personal data, and defines the responsibilities of staff and stakeholders.

2. SCOPE

This policy applies to:

- All staff, contractors, governors and volunteers
- All personal data processed by the College
- Data held on College systems and personal devices used for College business
- All formats of data, including digital, paper, audio, video and images

3. DATA PROTECTION PRINCIPLES

The College complies with the seven principles of UK GDPR:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

The College must be able to demonstrate compliance with these principles at all times.

4. LAWFUL BASIS FOR PROCESSING

The College processes personal data under one or more of the following lawful bases:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

Processing of Special Category Data requires an additional lawful condition under UK GDPR.

The lawful basis for processing is outlined in the College's Privacy Notices, which provide detailed information to individuals about how their data is used.

5. INDIVIDUAL RIGHTS

Individuals have the right to:

- Be informed about how their data is used
- Access their personal data
- Have inaccurate data corrected
- Have data erased (where applicable)
- Restrict processing
- Data portability
- Object to processing
- Not be subject to automated decision-making

The College ensures these rights are upheld in all processing activities.

6. PRIVACY NOTICES

The College maintains Privacy Notices which explain how personal data is collected, used, shared and retained.

Privacy Notices are provided to:

- Students and parents/carers
- Staff and job applicants
- Website users and other stakeholders

These notices include:

- The lawful basis for processing
- What data is collected
- How it is used and shared
- How long it is retained
- Individual rights

Privacy Notices are available on the College website and through internal systems.

7. FREEDOM OF INFORMATION

The College is committed to openness, transparency, and accountability and complies with the Freedom of Information Act 2000 (FOIA).

The Act provides members of the public with a general right of access to recorded information held by the College, subject to certain exemptions and exclusions defined by legislation.

The College will:

- maintain and publish information in accordance with the Information Commissioner's Office (ICO) Model Publication Scheme;
- respond to valid requests for information within the statutory timeframe of 20 working days;
- provide advice and assistance to applicants where appropriate;
- protect personal data and confidential information in accordance with data protection legislation and other legal obligations; and
- ensure that requests are handled consistently, fairly, and lawfully.

Requests for information should be submitted in writing to the College via the contact details published on the College website.

Where information cannot be disclosed, the College will explain the reason unless prohibited from doing so by law.

Individuals dissatisfied with the handling of a request may request an internal review and, if still dissatisfied, may complain to the Information Commissioner's Office.

Further information regarding Freedom of Information and the College Publication Scheme is available on the College website.

8. ROLES AND RESPONSIBILITIES

College Responsibilities

The College will:

- Maintain registration with the Information Commissioner's Office (ICO)
- Ensure policies and procedures are compliant and up to date
- Maintain records of processing activities (ROPA)
- Provide appropriate staff training
- Implement appropriate technical and organisational measures

Data Protection Officer (DPO)

The DPO will:

- Monitor compliance with data protection legislation
- Handle Subject Access Requests
- Investigate data breaches
- Provide advice and guidance
- Oversee DPIAs and risk assessments

Staff Responsibilities

All staff must:

- Comply with this policy
- Only access data necessary for their role
- Keep personal data secure
- Follow retention requirements
- Report suspected breaches immediately and no later than the same working day.
- Complete mandatory data protection training

9. DATA SECURITY

The College implements appropriate security measures, including:

- Access controls and permissions
- Encryption where appropriate
- Secure storage systems
- Secure disposal of data
- Staff awareness and training

Use of personal devices and remote working must comply with College IT and security policies.

10. DATA RETENTION

Personal data will only be retained for as long as necessary and in accordance with the College's Data Retention Schedule.

Data that is no longer required will be securely deleted or destroyed.

11. DATA PROCESSORS AND SHARING

Where third parties process data on behalf of the College:

- A written data processing agreement must be in place in accordance with UK GDPR Article 28.
- Appropriate security measures must be ensured
- Processing must follow College instructions

Data will only be shared where lawful, necessary and proportionate.

12. INTERNATIONAL DATA TRANSFERS

Personal data will only be transferred outside the UK where:

- The destination country has UK adequacy regulations, or
- Appropriate safeguards are in place (e.g. UK IDTA or UK Addendum)

All transfers must be approved by the Data Protection Officer.

13. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

The College will conduct DPIAs where processing is likely to result in a high risk to individuals, including:

- New systems or technologies
- Large-scale processing of sensitive data
- CCTV or monitoring systems

14. TRAINING AND AWARENESS

- All staff must complete data protection training at induction
- Refresher training must be completed annually
- Additional training will be provided for high-risk roles

APPENDIX A – SUBJECT ACCESS REQUEST (SAR) PROCEDURE

1. Receiving Requests:

    - Requests may be made verbally or in writing and must be forwarded to the DPO immediately.

2. Verification:

    - The identity of the requester must be verified before processing begins.

3. Timescales

    - Respond within 1 month
    - May extend by 2 months for complex requests
    - Clock starts once sufficient information is received

4. Processing the Request

    - Identify where data is held
    - Retrieve all relevant information
    - Redact third-party data where required
    - Ensure completeness

5. Providing the Response

    - Provide data securely
    - Ensure format is clear and accessible
    - Explain any withheld information

6. Recording

    - All SARs must be logged
    - Records retained for 6 years

APPENDIX B – DATA BREACH PROCEDURE

1. **Reporting**

    - All breaches or suspected breaches must be reported to the DPO immediately or no later than the same working day.

2. **Containment**
   Immediate steps must be taken to:

    - Stop the breach
    - Recover data where possible
    - Limit impact

3. **Risk Assessment**
   The DPO will assess:

    - Type and sensitivity of data
    - Number of individuals affected
    - Potential harm

4. **Notification**

    - ICO must be notified within 72 hours where required
    - Individuals must be notified if high risk

5. **Recording**
   All breaches must be recorded, including:

    - Nature of breach
    - Actions taken
    - Outcomes

6. **Review**
   Post-incident review must identify:

    - Root cause
    - Required improvements
    - Training needs

APPENDIX C – DATA RETENTION SCHEDULE

The College maintains a detailed Data Retention Schedule which outlines how long personal data is retained and when it must be securely disposed of.

The schedule includes:

- Student records
- HR and payroll records
- Finance records
- Safeguarding records
- Governance records
- Estates and health and safety
- IT systems

Key Principles

Staff must ensure:

- Data is retained only as long as necessary
- Retention periods are applied consistently
- Data is securely destroyed when no longer required
- Exceptions are approved by the Data Protection Officer

Example Retention Periods

- Student records: End of relationship + 6 years
- Safeguarding records: Until age 25 (or longer if required)
- HR records: Up to 6 years after employment
- Pension records: Up to age 100

Full details are contained in the Retention Schedule spreadsheet.

Responsibilities

- Staff apply retention rules in their areas
- Managers ensure compliance
- The Data Protection Officer provides oversight and guidance

GLOSSARY OF TERMS

Personal Data
Information relating to an identified or identifiable individual, such as name, identification number, location data or online identifier.

Special Category Data
Personal data that is more sensitive and requires additional protection, including information about health, ethnicity, religion, political opinions, biometric data or sexual orientation.

Data Subject
The individual to whom personal data relates.

Processing
Any operation carried out on personal data, including collection, storage, use, sharing, or deletion.

Data Controller
The organisation that determines the purposes and means of processing personal data. The College is the Data Controller.

Data Processor
A person or organisation that processes personal data on behalf of the Data Controller.

Data Protection Officer (DPO)
The individual responsible for overseeing data protection compliance, advising on obligations, and acting as a contact point for the ICO.

Data Breach
A security incident that results in accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to personal data.

UK GDPR
The UK General Data Protection Regulation, which governs how personal data must be processed in the United Kingdom.

Data Protection Act 2018
UK legislation that sits alongside UK GDPR and sets out additional data protection rules.

Lawful Basis
The legal reason for processing personal data under UK GDPR (e.g. consent, contract, legal obligation, public task).

Consent
A freely given, specific, informed and unambiguous indication of a data subject's wishes by which they agree to the processing of their personal data.

Public Task
Processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

Legitimate Interests
Processing necessary for the legitimate interests of the organisation or a third party, balanced against the rights of the individual.

Privacy Notice
A document that explains how personal data is collected, used, shared and retained, and outlines individuals' rights.

Subject Access Request (SAR)
A request made by an individual to access the personal data held about them.

Data Protection Impact Assessment (DPIA)
A process used to identify and minimise data protection risks in high-risk processing activities.

Record of Processing Activities (ROPA)
A document that records what personal data is processed, why it is processed, how it is used, and how long it is retained.

Retention Period
The length of time personal data is kept before it is securely deleted or destroyed.

Data Sharing
The disclosure of personal data to a third party, either within or outside the organisation.

International Data Transfer
The transfer of personal data outside the United Kingdom.

Information Commissioner's Office (ICO)
The UK's independent authority responsible for upholding information rights and enforcing data protection law.