The College of Animal Welfare

Data Protection Policy and Procedure

Version 1.1

1. Introduction

The College of Animal Welfare ("the College") is committed to protecting the privacy and rights of all learners, apprentices, applicants, staff, governors, employers and visitors. We comply with the United Kingdom General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). We also ensure our data processing supports statutory safeguarding duties, including Keeping Children Safe in Education (KCSIE), Working Together to Safeguard Children and the Prevent Duty guidance.

This policy sets out how we collect, use, share, protect and retain personal data; how we uphold information rights; and how our data protection arrangements underpin expectations for safeguarding, inclusion, equality and diversity across the College.

2. Scope and Purpose

This policy applies to all personal data processed by or on behalf of the College, regardless of format (paper, digital, audio-visual) or location (on-site, remote, cloud). It covers all activities undertaken in connection with teaching, learning, apprenticeships, placements, student support, safeguarding, HR, finance, marketing, research and governance.

3. Roles and Responsibilities

Data Controller: The College as a corporate body is the Data Controller for personal data it processes. The Principal and Senior Leadership Team are accountable for compliance.

Data Protection Officer (DPO): The Vice Principal Corporate Services is designated as the College's DPO and oversees compliance, advises on data protection law, monitors risks, and acts as the primary contact for the Information Commissioner's Office (ICO). A named deputy will act when the DPO is unavailable.

Designated Safeguarding Lead (DSL): Works jointly with the DPO to ensure safeguarding records and information sharing are managed lawfully, proportionately and securely.

Managers: Ensure staff and contractors understand and follow this policy and related procedures in their areas.

All Staff and Contractors: Must complete mandatory training, handle personal data lawfully and securely, and report any personal data breach or near miss immediately via the College's incident reporting process.

4. Lawful Bases and Special Category Data

We process personal data under one or more lawful bases in Article 6 UK GDPR, including public task, contract, legal obligation, vital interests, consent and legitimate interests (where applicable). For special category data (Article 9) and criminal offence data (Article 10/DPA 2018), we apply

appropriate policy safeguards and an additional lawful condition in Schedule 1 DPA 2018 e.g. employment, social protection, safeguarding of children and individuals at risk.

5. Data Protection Principles

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability: the College shall be responsible for, and able to demonstrate, compliance

6. Safeguarding, Prevent and Information Sharing

We recognise that effective safeguarding depends on timely and proportionate information sharing. Where there is a safeguarding concern, we will share personal data with appropriate agencies e.g. local authority children's services, police, health, Channel/Prevent partners or the Disclosure and Barring Service, when it is lawful and necessary to protect a child or vulnerable adult, prevent harm, or meet statutory duties. We rely on the most appropriate lawful basis, including vital interests, legal obligation, public task, or substantial public interest conditions under the DPA 2018.

Safeguarding records are restricted to authorised safeguarding staff and retained securely in line with our Safeguarding Policy and KCSIE. The DPO and DSL review safeguarding data processes at least annually to assure compliance and continuous improvement.

7. Inclusion, Accessibility and Equality

We comply with the Equality Act 2010 and the Public Sector Equality Duty. We will ensure our data protection processes do not discriminate against individuals with protected characteristics and will take reasonable steps to provide accessible formats, assistive technologies and communication support for privacy notices and requests e.g. subject access requests.

We use data responsibly to identify and reduce barriers to participation and outcomes for learners, including those with SEND, those who are disadvantaged, apprentices, adults and those facing other vulnerabilities. Findings inform targeted support and inclusive practice across the College.

8. Fair Processing and Transparency

We publish clear privacy notices for learners, applicants, staff, employers and visitors explaining what data we collect, why we collect it, our lawful bases, who we share it with, retention periods,

international transfers, and how to exercise rights. Where appropriate, we will provide notices in accessible formats.

9. Data Security and Access Control

We apply appropriate technical and organisational measures to protect personal data, including role-based access controls, multi-factor authentication for key systems, encryption of portable media, device management, secure configuration, logging and monitoring, and secure disposal of paper and electronic records.

Staff must not store College personal data on personal devices or consumer cloud services. Paper records must be kept in lockable storage and disposed of via confidential waste or approved shredding.

10. Records Management and Retention

We maintain Records of Processing Activities (ROPA) and retention schedules. Retention periods are based on legal requirements and business need. Safeguarding records are retained in line with KCSIE and our Safeguarding Policy; HR, finance and learner records follow sector guidance and statutory requirements. Where specific legal requirements change, we will update our schedules accordingly.

11. Data Protection Impact Assessments (DPIAs)

We complete DPIAs for high-risk processing, including new systems, large-scale processing of special category data, systematic monitoring (e.g. CCTV), online safety/monitoring tools, or international data transfers. The DPO must be consulted at an early stage.

12. Data Processors and Third-Party Sharing

We only appoint processors who provide sufficient guarantees of compliance. Contracts include Article 28 UK GDPR clauses covering confidentiality, security, sub-processing, audit rights and deletion/return of data. International transfers are subject to Transfer Risk Assessments and appropriate safeguards (e.g. UK IDTA or EU SCCs plus UK Addendum).

13. CCTV, Images and Recordings

We operate CCTV and capture photographs/recordings for specified purposes set out in relevant privacy notices. We will display signage where CCTV is in use, limit access to authorised staff, and apply proportionate retention. Where consent is required e.g. marketing images, it will be informed, recorded and can be withdrawn without detriment.

14. Individual Rights

- Right to be informed (privacy notices)
- Right of access (Subject Access Requests)
- Right to rectification
- Right to erasure (where applicable)
- Right to restrict processing
- Right to data portability (where applicable)
- Right to object (including to direct marketing)
- Rights related to automated decision-making and profiling

We will respond to requests without undue delay and within one month. Where requests are complex or numerous, we may extend by up to two further months and will inform the requester within one month. We will verify identity where necessary and provide information in accessible formats on request.

15. Subject Access Requests (Procedure)

Requests can be made in any format to the DPO. We will: (a) verify identity, (b) clarify scope, (c) search relevant systems, (d) consider third-party data and applicable exemptions (e.g. prevention/detection of crime; management forecasts; confidential references; exam materials; safeguarding where disclosure would risk harm), and (e) provide copies securely.

16. Personal Data Breaches (Procedure)

All suspected personal data breaches must be reported immediately via the incident process. The DPO will assess risk, contain the incident, record it in the breach log, and notify the ICO within 72 hours where required. Where there is a high risk to individuals, we will notify affected data subjects without undue delay, describing the nature of the breach, likely consequences and measures taken.

17. Training and Awareness

All staff and contractors' complete induction and periodic refresher training on data protection, information security, safeguarding information sharing, Prevent and equality duties. Additional role-specific training is provided to those handling high-risk data e.g. HR, safeguarding, IT, quality.

18. Governance, Assurance and Audit

The DPO provides an annual data protection assurance report to the Advisory Board and Principal, including breach trends, ROPA updates, DPIA outcomes, SAR metrics, equality/accessibility

considerations and improvement actions. Internal audit and external assurance may be used to test compliance.

19. Complaints and Contact

Questions, requests or complaints should be directed to the DPO: Vice Principal Corporate Services (contact details published on the College website and VLE). Individuals may also complain to the ICO.

20. Review

This policy and procedures will be reviewed at least annually and after any significant change in legislation, regulation, Ofsted requirements or College operations.

Appendix A

Subject Access Request (SAR) form (short)

Name:

Email/Phone:

Address:

Details of information requested (including relevant dates and systems):

I understand the College may need to verify my identity and may lawfully redact third-party data or apply exemptions.

Signature:

Date:

Appendix B

High-level Retention Guidance (extract)

- Safeguarding records – retained in line with KCSIE and the College Safeguarding Policy (longer than standard records where appropriate)
- HR records – in line with statutory requirements and limitation periods (e.g. payroll, tax, grievance/disciplinary)
- Learner records – minimum periods to meet funding, awarding body and limitation requirements; longer for transcripts/references where agreed
- CCTV/images – proportionate retention (typically short duration) unless required for investigation.

Date Policy Reviewed	March 2026
Version	v1.1
Policy Owner	Barbara Cooper
Next review due	March 2027