Wiltshire College

Data Protection Policy

Agreed SLG May 2018

To be reviewed May 2019

Contents **Page**

1. Scope and Purpose

This policy sets out the principles by which Wiltshire College collects, handles and stores personal data in accordance with the college's standards and to comply with the law.

Wiltshire College only collects, handles and stores the personal data it needs to conduct its operations as a Further Education College business or where it is required to do so by government agencies.

The policy applies to all college staff in all of its sites and operations. Everyone has some level of responsibility for ensuring that personal data is collected, handled and stored appropriately and in compliance with the law.

The policy applies to all data it holds relating to identifiable individuals.

Personal data is any information relating to a living, identifiable person **who can be identified by** reference to an identifier or in conjunction with other information that is held. It includes things such as name, address, email address (including email addresses of individuals in companies), IP address and also more sensitive types of data, called Special categories of personal data.

Special categories of personal data – this is personal data that gives a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, physical or mental health, sexual life, sexual orientation and criminal record. Special Categories of personal data are subject to additional controls.

The purpose of the policy is to set out how Wiltshire College

- Complies with data protection law and follows good practice
- Protects the rights of its staff, students, partners and any organisation or individual with which it does business
- Is open about how it stores and processes individuals data
- Protects itself from the risks of a data breach

2. Accountability

All staff are responsible for compliance with this policy. The policy helps to protect Wiltshire College from data security risks including:-

- Breaches of confidentiality
- Processing personal data for which active consent has not been obtained
- Reputational damage as a result of poor data protection practice or data breaches

Everyone who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles, but the following people or groups have key areas of responsibility:

- The Corporation Board (Governing Body) is the ultimate decision-making authority of the college and is responsible for its overall strategic direction and its legal compliance. It ensures that appropriate processes and procedures are in place to achieve such compliance. Governors conduct themselves in accordance with accepted standards of behaviour in public life.
- The Data Protection Officer is responsible to the Board for data protection compliance. The post of Clerk to the Corporation has been designated as the Data Protection Officer as it is fulfils the necessary criteria for the role being separate from the management structure of the College, it reports to the Board and the post holder will have knowledge and experience of compliance, knowledge of the organisation and the authority to carry out the role.

- The Senior Leadership Group is responsible for the executive management of the College and has responsibility for the structure for data processing, to ensure that appropriate resources are provided to enable good data protection and that staff comply with this policy.
- The Director of Funding and Learning Resources is responsible to the Senior Leadership Group for data protection and control. The post-holder is responsible for maintaining a record of all categories of personal data processing activities carried out on behalf of the college as a data controller and processor.
- The Director of ICT Services is responsible for the technology provided by the college to achieve data protection by design.
- The Head of Teaching, Learning and Assessment is responsible for the main teaching, learning and assessment activities of the college and the organisational systems which support these activities including the handling of personal data as part of these.
- The Marketing and Communications Manager is responsible for personal data processing of customers' details and also for the framework and content of the college website which is the main means of communication to the public and to college users of information about data protection.
- The Exams and Compliance Manager has day to day responsibility for maintaining the record of personal data processing and also for tracking responses to subject access requests.

3. Policy Statement

Wiltshire College will process personal data lawfully, fairly and transparently. It will collect data for specified, explicit and legitimate purposes and will process it in line with those purposes. Personal data collection will be adequate, relevant, limited to what is necessary for the purposes intended and only kept for as long as is required for these purposes. It aims to ensure that personal data held is accurate and is kept up to date and to take every reasonable step to ensure that where the information held is inaccurate that it is removed or put right without delay. The College takes the security of personal data seriously and will take steps to protect it against unauthorised or unlawful processing and against accidental loss, destruction or damage. The College supports the principle of securing personal data by design.

4. Processes and Principles

4.1 *General Guidelines*

- *Access* – Personal data will only be available to staff who are entitled to access it for lawful and legitimate work purposes.
- *Data protection by design* – The College will seek to build in data protection by design in all its practices. It recognises that privacy by design is a requirement.

- *Lawful purpose for processing*– The College will only collect, hold and process personal data where it has a lawful purpose for doing so. Where the basis for lawful processing is consent the College will only hold and process personal data where it has confirmed the active consent of an individual to do this. A list of lawful purposes for processing has been identified, which is given as an appendix to this policy.
- *Training* – General training will be provided to all staff in relation to data protection and participation is mandatory. This will be addressed in the induction of all staff and training will be given to enable all staff to understand their responsibilities when handling personal data. Where a member of staff's role may require specific training, this will be provided.
- *Assistance and guidance*- Staff should request help from their line manager in the first instance if they are unsure of any aspect of data protection. Where required, staff and line managers will have access to the Director of Funding and Learning Resources for organisational support and the Data Protection Officer where general guidance is required. The College will provide a series of Best Practice Guides to staff to cover aspects of work and expected behaviour relating to good data protection principles. The current list of topics covered in Best Practice Guides is available on the college's internal intranet.
- *Resources* – A programme of resources to support data protection will be introduced and maintained by the college.

4.2 Consent – Where consent is required from an individual to handle their personal data, this will be clear and recorded. This consent can be withdrawn at any time and is made clear to individuals. Care will be taken to ensure that records are kept accurately to show consent. Individuals are entitled to have their data deleted if they request this. Where data is provided by consent, an individual has a right to be forgotten.

4.3 Data Storage – The College is committed to keeping all data stored securely. Features to protect personal data by technology design will be used by the college such as password protection and data encryption. Physical measures will be used where appropriate such as locked filing cabinets, locked rooms. The College has conducted a comprehensive data audit of how all its personal data is stored. This will be reviewed and updated regularly.

4.4 Data Usage and grounds for data processing – Personal data will only be used and kept where is needed for the college's lawful purposes. A full analysis of the lawful purposes for the processing of personal data has been undertaken and is published on the College website.

4.5 Data accuracy – The College takes care to ensure that all data it holds is accurate. It checks this with individuals when it is originally collected. Should a student think that their personal information held is not accurate they should notify Student Services. Staff should notify Human Resources. If their circumstances change, such as a change of address or name, students should inform Student Services and staff should notify Human Resources. The College will take action immediately to correct personal data when it has been informed that it is not accurate.

4.6 Data disclosure – The College will only disclose personal data to other organisations where it has informed individuals that their personal information will be shared and where data sharing agreements with those organisations are in place. Students are informed as

part of their enrolment about the organisations with whom the College shares data and the reasons why data sharing may take place and consent will be requested.

4.6 *Privacy statements* – A privacy statement will be included on all forms that collect information about potential students, students, staff and governors. This includes the College's CCTV policy.

4.7 *Privacy impact assessments* – The circumstances where an impact assessment is required will be kept carefully under review. These will explicitly cover aspects such as how the data is retained securely and for what period.

4.8 *Subject Access requests* – The College fully recognises and supports the rights of individuals to make a subject access request. Information about the best way to make a request is included on the Data Protection section of the college website. It will help requests to be processed promptly where they are emailed to subjectaccessrequest@wiltshire.ac.uk The College expects to answer all subject access requests within the 28 day deadline.

4.8 *Reporting data security breaches* – The College views data protection of great importance and will treat any data security breach as a matter of urgency. The risks associated with a breach are included in the College's Risk Register. When it becomes aware of a breach it will notify the Information Commissioner and identified affected individuals within 72 hours and sooner wherever possible. Staff and students must notify the Data Protection Officer immediately if they suspect that a data breach has taken place. The College has prepared a separate process for the handling of data security breaches including how they may be detected, how they should be reported and how they will be investigated. This process is attached to this policy as an appendix and will be placed on the college website.

4.9 *Website information* – The College will have a prominent section on its website where information about data protection will be held. This will be straightforward and clear and will be a main source of information for individuals about data protection.

5. Implementation

The Data Protection Policy is a key policy to be acknowledged by all staff. This policy will be implemented through training, publicity to staff and through the website. It will be supported through the use of spot checks and audits and there will be regular reporting to Managers. Governors will receive at least an annual report on data processing compliance and activity as well as other reports from time to time where there are particular developments to be reported or decisions required.

6. Associated Documents

Other relevant documents related to this policy include the Information Systems and Acceptable Use policy, Disciplinary policies, Complaints Policy, Equality and Diversity Policy and Safeguarding Policy.

7. Equality Impact Assessment

An equality impact assessment has been carried out in relation to this policy.

8. Data Impact Assessment

All considerations of data protection have been considered in the preparation of this policy. All other college policies will take account of this policy.

Appendix 1

Data Breach Notification Procedure - WILTSHIRE COLLEGE

Where there is a data breach within the College, it is a legal requirement to notify the Information Commissioner Officer (ICO) within 72 hours and the individuals concerned as soon as possible in certain situations. It is essential therefore that all data breaches, no matter how big or small, are reported to College management.

This Procedure should be read in conjunction with our Data Breach Policy and Data Protection Policy. Our Data Breach Policy contains detailed information on what constitutes a data breach; please read it to make sure that you understand about this.

This Procedure should be followed by all staff. At all stages of this procedure, our Data Protection Officer and management will decide whether to seek legal advice. This procedure will also apply where we are notified by any third parties that process personal data on our behalf that they have had a data breach which affects our personal data.

The procedure is set out below. Any failure to follow this procedure may result in disciplinary action.

Your main responsibilities as a member of staff are to:

- ***Inform*** your line manager or the Data Protection Officer as soon as you discover or suspect a data breach
- ***Assist*** with any investigation, but only where you are asked to do so
- ***NOT TO TRY TO DEAL WITH THE DATA BREACH YOURSELF***

IDENTIFYING AND REPORTING A DATA BREACH
If you discover a data breach, however big or small, you must report this to our Data Protection Officer immediately. The Data Protection Officer is the Clerk to the Corporation, Heather Cross, and can be contacted via: extension - 3450, and email address dataprotectionofficer@wiltshire.ac.uk . Any other questions about the operation of this procedure or any concerns that the procedure has not been followed should be referred in the first instance to the Data Protection Officer. A data breach could be as simple as you putting a letter in the wrong envelope and therefore even the most minor data breaches ***must*** be reported. False alarms or even breaches that do not cause any harm to individuals or to the College should nevertheless be reported as it will enable us to learn lessons in how we respond and the remedial action we put in place. We have a legal obligation to keep a register of all data breaches, no matter how big or small and no matter whether any harm was caused. Please ensure that you do report any breach, even if you are unsure whether or not it is a breach.

BECOMING AWARE OF A DATA BREACH – INVESTIGATING

We become aware of a data breach when we have a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. From this point, our time limit for notification to the ICO will commence.

When you report a data breach to our Data Protection Officer, our Data Protection Officer will promptly investigate the breach to ascertain whether we are fully aware that a breach has occurred that has led to personal data being compromised.

THIS WILL BE DONE WITHIN 24 HOURS OF A BREACH BEING REPORTED TO US.

ASSESSING A DATA BREACH

Once you have reported a breach and our Data Protection Officer has investigated it and has decided that we are aware that a breach has occurred, our Data Protection Officer will log the breach in our Data Breach Register and will carry out an initial assessment of the breach to evaluate its severity.

Once the level of severity is known, our Data Protection Officer will notify management. If necessary, we will appoint a response team which may involve for example our HR and IT teams and we will assign responsibility for particular tasks as necessary across the response team.

We will then investigate the breach and consider any on-going risks to the College and any individuals affected.

If our Data Protection Officer and management consider that the breach is very serious, they will consider the impact on our reputation and the effect it may have on the trust placed in us. Our Data Protection Officer and senior management will consider whether to appoint a PR professional to advise on reputational damage and will also consider whether legal advice is needed.

THIS WILL BE DONE WITHIN 24 HOURS OF US BECOMING AWARE OF THE BREACH.

FORMULATING A RECOVERY PLAN

Our Data Protection Officer and senior management will investigate the breach and consider a recovery plan to minimise the risk to individuals. As part of the recovery plan, our Data Protection Officer and senior management may interview any key individuals involved in the breach to determine how the breach occurred and what actions have been taken.

THIS WILL BE DONE WITHIN 24 HOURS OF ASSESSING THE BREACH.

NOTIFYING A DATA BREACH TO THE ICO

Unless the breach is unlikely to result in a risk to the rights and freedoms of individuals, we must notify the breach to the ICO within **72 hours** of becoming aware of the breach. We must also notify the individuals concerned as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.

The content of the notification will be drafted by our Data Protection Officer in line with our Data Breach Policy, and the notification will be made by our Data Protection Officer – please be aware that **under no circumstances must you try and deal with a data breach yourself**.

THIS WILL BE DONE WITHIN 72 HOURS OF BECOMING AWARE OF THE BREACH.

NOTIFYING A DATA BREACH TO INDIVIDUALS

We must also notify the individuals concerned as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.

The content of the notification will be drafted by our Data Protection Officer in line with our Data Breach Policy and in conjunction with consulting the ICO if considered necessary. We will notify individuals in clear and plain language and in a transparent manner (for example by email, SMS or letter). Please be aware that **under no circumstances must you try and deal with a data breach yourself.**

In some circumstances, explained in our Data Breach Policy, we may not need to notify the affected individuals. Our Data Protection Officer will decide whether this is the case.

THIS WILL BE DONE AS SOON AS POSSIBLE AFTER WE BECOME AWARE OF THE BREACH.

NOTIFYING A DATA BREACH TO OTHER RELEVANT THIRD PARTIES

We may also consider that it is necessary to notify other third parties about the data breach depending on the nature of the breach. This could include:

- Insurers
- Police
- Employees
- Parents/Guardians
- Sponsors
- Banks
- Contract counterparties

The decision as to whether any third parties need to be notified will be made by our Data Protection Officer and management. They will decide on the content of such notifications.

THIS WILL BE DONE WITHIN 5 DAYS OF BECOMING AWARE OF A DATA BREACH.

Note: We suggest that a time frame is included. We suggest a timeframe of 5 days. Please do amend this time frame as you

CONSIDER WHETHER NOTIFICATIONS NEED TO BE UPDATED

We need to keep the ICO up to date about the data breach. If anything changes from the time we send the initial notification to the ICO, our Data Protection Officer will consider whether we need to update the ICO about the data breach.

THIS WILL BE CONSIDERED ON AN ONGOING BASIS.

EVALUATION AND RESPONSE

The key to preventing further incidents is to ensure that the College learns from previous incidents.

It is extremely important to identify the actions that the College needs to take to prevent a recurrence of the incident. Our Data Protection Officer and management will carry out an evaluation as to the effectiveness of our response to the data breach and document this in our Data Breach Register.