Honiton Community College

Academy Trust

DATA PROTECTION POLICY

This Policy was adopted by the Governing Body of

Honiton Community College Academy Trust

on 5th October 2016

and will be reviewed every two years

Senior Information Risk Officer (SIRO): Andy Holt

Data Protection Policy

Introduction

The Data Protection Act 1998 (DPA 1998) establishes a framework of rights and duties which safeguard personal data. Personal data is information about a living individual, who can be identified from the data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes, against the right of individuals to respect, for the privacy of their personal details.

Honiton Community College Academy Trust is committed to protecting the privacy of individuals and handles all personal data in a manner that complies with the DPA 1998. The College has established the following policy to support this commitment. It is the **personal responsibility** of all employees (temporary or permanent), Members, contractors, agents and anyone else processing information on our behalf to comply with this policy. This policy continues to apply to employees and individuals, even after their relationships with the College ends.

Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation, for example the Computer Misuse Act 1990 and the DPA 1998. All incidents will be investigated and action may be taken under the College's formal disciplinary procedure. A serious breach of this policy could be regarded as gross misconduct and may lead to dismissal and/or criminal action being taken.

This policy explains what our expectations are when processing personal data.

Data Protection Principles

1.1 The DPA 1998 is underpinned by a set of eight common-sense principles, which must be adhered to whenever personal data is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal data.

A summary of the data protection principles is as follows:
Personal data must be:

- Processed fairly and lawfully
- Processed for specified and lawful purposes
- Adequate, relevant and not excessive
- Not kept longer than is necessary
- Processed in accordance with the rights of the data subject
- Kept secure
- Transferred only to countries with adequate security

2. Access and use of Personal Data

2.1 Access and use of personal data held by the College is only permitted by employees (temporary or permanent), Members, contractors, agents and anyone else processing information on our behalf, for the purpose of carrying out their official duties. Use for any other purpose is prohibited.

2.2 Deliberate unauthorised access to, copying, disclosure, destruction or alteration of or interference with any computer equipment or data is strictly forbidden and may constitute a criminal and/or a disciplinary offence.

2.3 It is an offence under Section 55(1) of the Data Protection Act, for any person to knowingly or recklessly obtain, procure or disclose personal data, without the permission of the data controller (Honiton Community College Academy Trust) subject to certain exceptions.

2.4 It is also an offence for someone to sell or offer to sell personal data which has been obtained in contravention of Section 55(1). Full details of this offence can be found under Section 55 of the Data Protection Act 1998.

3. Collecting Personal Data

3.1 When personal data is collected, for example on a questionnaire, survey or a form, the data subject (that is to say the person who the information is about) must be told, unless this is obvious to them, which organisation(s) they are giving their information to; what their information will be used for; who it may be shared with and anything else that might be relevant e.g. the consequences of that use. This is known as a Privacy Notice.

3.2 Personal data collected, must be adequate, relevant and not excessive for the purpose of the collection. A person's name and other identifying information should not be collected where depersonalised (anonymous) information would suffice.

3.3. If the information is collected for one purpose, it cannot subsequently be used for a different and unconnected purpose, without the data subject's consent (unless there is another lawful basis for using the information (see section 4 below)). It must be made clear to the data subject at the time the information is collected, what other purposes their information may be used for.

4. Lawful Basis for Processing

4.1 When Honiton Community College Academy Trust processes personal data, it must have a lawful basis for doing so. The DPA 1998 provides a list of 'conditions' when we can process personal or 'sensitive' personal data and are contained within Schedule 2 and Schedule 3 of the Act.

4.2 The DPA 1998 defines 'sensitive' personal data as information relation to a person's racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health or condition; sexual life; criminal offences (alleged or committed).

4.3 Whenever the College processes personal data, it must be able to satisfy at least one of the conditions in Schedule 2 of the DPA 1998 and when it processes 'sensitive' personal data; it must be able to satisfy at least one of the conditions in Schedule 3 of the DPA 1998 as well.

4.4 As an example, Honiton Community College Academy Trust can process personal data if it:

- Is necessary to comply with a legal obligation
- Is necessary to protect someone's life or to protect them from serious harm
- Is in the public interest and is necessary for Honiton Community College Academy Trust or another organisation to undertake its official duties
- Is necessary for a legitimate and lawful purpose and does not cause unwarranted prejudice to the data subject
- Is necessary to assist in the prevention or detection of an unlawful act

4.5 The College can also process personal data if it has the data subject's consent (this needs to be 'explicit' when it processes sensitive personal data). In order for consent to be valid it must be 'fully informed' which means the person giving consent must understand what they are consenting to and what the consequences are if they give or refuse consent. Consent must not be obtained through coercion or under duress.

5. Disclosing Personal Data

5.1 Personal data must not be disclosed to anyone internally or externally, unless the person disclosing the information is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled to the information.

5.2 If the personal data is disclosed to another organisation or person outside of the College, the disclosing person must identify their lawful basis for the disclosure (see Section 4 above) and record their decision. This should include a description of the information disclosed; the name of the person and organisation the information was disclosed to, the date, the reason for the disclosure and the lawful basis.

5.3 In response to any lawful request, only the minimum amount of personal information should be disclosed. The person disclosing the information should ensure that the information is adequate for the purpose of the disclosure, relevant and not excessive.

5.4 When personal data is disclosed internally or externally, it must be disclosed in a secure manner.

6. Accuracy and Relevance

6.1 It is the responsibility of those who receive personal information to ensure so far as possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to ensure that it is still accurate. If the information is found to be inaccurate, steps must be taken to rectify it. Individuals who input or update information must also ensure that it is adequate, relevant, unambiguous and professionally worded. Data subjects have a right to access personal data held about them and have inaccuracies corrected. More information about a data subject's rights can be found in Section 8 below.

7. Retention and Disposal of Data

7.1 Honiton Community College Academy Trust holds a vast amount of information. The DPA 1998 requires that we do not keep personal data for any longer than is necessary. Personal data should be checked at regular intervals and deleted or destroyed when it is no longer needed, provided there is no legal or other reason for holding it.

7.2 Information, equipment or media must be disposed of in a secure way.

8. Individual's Rights

8.1 Individuals have several rights under the DPA 1998. These include the right to access personal data held about them (this is known as Subject Access); the right to prevent their information being used in a way which is likely to cause damage or distress; the right to compensation for any damages as a result of their information not being handled in accordance with the DPA 1998; and the right to have inaccurate or misleading information held about them, corrected or destroyed. A person wishing to exercise any of these rights must produce a written request to the Principal.

8.2 It is particularly important that if a person has made a Subject Access request that this is forwarded to the Principal as soon as possible. The College has 40 calendar days in which to respond to a Subject Access request, provided the applicant has put their request in writing and suitable identification has been supplied.

9. Reporting Security Incidents

9.1 Honiton Community College Academy Trust has a responsibility to monitor all incidents that occur within the organisation that may breach the security and/or the confidentiality of its information. All incidents need to be identified, reported, investigated and monitored. It is only by adopting this approach that the College can learn from its mistakes and prevent losses re-occurring.

9.2 The College requires any staff to report if information has been lost, found or stolen (including the loss or theft of laptops, Blackberries, Smartphones, etc) this must be reported to the Senior Information Risk Officer in writing (Please see Appendix 1 for 'The Role of the Senior Information Risk Officer (SIRO)).

Appendix 1

The Role of the Senior Information Risk Officer (SIRO)

1. Background

1.1 The establishment of the role of SIRO is one of several measures to strengthen controls around information security outlined in a recent Cabinet Office review and report on Data Handling. The SIRO will be a member of the Executive Leadership Team (ELT) of the Academy Trust who is familiar with information risks and the organisation's response to risk and has the knowledge and skills necessary to provide the required input and support to the Board and to the Accountable Officer.

2. Accountability and Performance

2.1 Executive level ownership of information risk is a key factor in successfully raising the profile of information risks and to embedding information risk management into the overall risk management culture of the Academy Trust. Executive leadership demonstrates the importance of the issue and is critical in obtaining the resources and commitment necessary to ensuring information security remains high on the Board agenda.

3. The role of the Accountable Officer

3.1 The Principal, as Accounting Officer of the Academy Trust, has overall accountability and responsibility for Information Governance in the Trust and is required to provide assurance, through the Statement of Internal Control, that all risks to the Trust, including those relating to information, are effectively managed and mitigated.

4. The role of the Senior Information Risk Officer (SIRO)

4.1 The SIRO will be a member of the ELT.

4.2 The SIRO will be expected to understand how the strategic business goals of the Academy Trust may be impacted by information risks.

4.3 The SIRO will act as an advocate for information risk on the Governing Body and in internal discussions, and will provide written advice to the Accountable Officer on the content of their annual Statement of Internal Control in regard to information risk.

4.4 Working within a simple governance structure, with clear lines of ownership and well defined roles and responsibilities, the SIRO will provide an essential role in ensuring the identified information security threats are followed up and incidents managed. They will also ensure that the Governing Body and the Accountable Officer are kept up-to-date on all information risk issues.

5. Key responsibilities of the SIRO

5.1 To oversee the development of a Data Protection Policy, and a Strategy for implementing the policy within the existing Information Governance Framework.

5.2 To take ownership of the risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal

Control.

5.3 To review and agree an action plan in respect of identified information risks.

5.4 To ensure that the Trust's approach to information risk is effective in terms of resource,

commitment and execution and that this is communicated to all staff.

5.5 To provide a focal point for the resolution and/or discussion of information risk issues.

5.6 To ensure the Governing Body is adequately briefed on information risk issues.