Halesowen College

Data Protection Policy

Introduction

Halesowen College needs to collect and use certain types of information about people with whom it deals in order to operate. These include current, past and prospective employees and students, suppliers, customers, stakeholders and others with whom it communicates. In addition, it may occasionally be required by law to collect and use certain types of information of this kind to comply with the requirements of government departments. Any such information, whether deemed confidential or not, relating to a living individual who can be identified from that information (or from that information or other data in the College's possession), and which may be factual (such as name, address or date of birth) or an opinion (such as a performance appraisal) is subject to data protection laws (and is referred to as "personal data" in this Policy, the Data Protection Procedures and its Appendices). This personal data must be dealt with properly however it is collected, recorded and used – whether on paper or digitally. This policy describes how this personal data must be collected, handled and stored. As such, this policy ensures:

- compliance with the law and best practice
- protection of the rights of staff
- students, partners et al
- openness about processing and storage of data
- avoidance of risk of a data breach

In accordance with the Data Protection Act 1998 (referred to in this Policy, the Data Protection Procedures and its Appendices as "the Act") and associated EU Directives, Halesowen College will handle personal data in a manner which complies with the eight Data Protection Principles specified under the Act regarding privacy and disclosure (see Data Protection Principles in Appendix 1 of Data Protection Procedures).

The lawful and correct treatment of personal data by Halesowen College is very important to successful operations, and in maintaining confidence between those with whom the College interacts. Halesowen College therefore ensures personal data is treated lawfully and correctly, recorded accurately, kept up to date, stored securely and used for the intended purpose. Whilst the Act does not guarantee personal privacy it aims to strike a balance between the rights of the individual and requirements of the organisation.

The Act allows individuals to find out what personal data is held about them by making a subject access request. This covers information held electronically and in some paper records. Individuals have the right to obtain personal data in an electronic and structured form which allows further use by the individual[1].

If individuals think they are being prevented from seeing information they are entitled to, they can ask the Information Commissioner to help. The Information Commissioner's Office is responsible for looking after rights of individuals and making sure personal data is not misused.

[1]Data Protection Law allows for individuals to exercise their 'right to be forgotten' with personal information being erased where it is no longer necessary for the purpose for which it was processed or where the data subject withdraws consent or otherwise objects to the processing. In such cases the College would action this and then take reasonable steps to inform third parties

Halesowen College is registered with the Information Commissioner and all registrations under the Act are reviewed annually for accuracy and completeness by the College.

Halesowen College has a Data Protection Officer and maintains records/registers of data processing activity.

The Data Protection Principles

Halesowen College endorses and will adhere to the Principles of data protection, as established in the Data Protection Act 1998. The College recognises that failure to hold and process information in a fair and proper way may ultimately lead to a criminal offence being committed.

Specifically, the Principles require that personal data:

i shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;

ii shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;

iii shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;

iv shall be accurate and, where necessary, kept up to date;

v shall not be kept for longer than is necessary for that purpose or those purposes;

vi shall be processed in accordance with the rights of data subjects under the Act;

and that:

vii appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (see data security guidelines);

viii shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Code of Practice

Halesowen College *will*, through appropriate management, and strict application of criteria and controls:

- observe fully conditions regarding the fair collection and use of information (see section on fair processing);
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the accuracy and quality of information used;
- apply strict checks to determine the length of time information including images is held;

- ensure that the rights of people about whom information is held can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken; the right of access to one's personal data; the right to prevent processing in certain circumstances; the right to correct rectify, block or erase information which is regarded as wrong information);
- take appropriate technical and organisational security measures to safeguard personal data;
- ensure that personal data is not transferred outside the EEA without suitable safeguards.
- observe and understand the exemptions from the Act.

In addition, Halesowen College will ensure that:

- there is someone with specific responsibility for data protection in the organisation (currently, CIS Manager ext 264) who acts as the Data Protection Officer;
- everyone managing and handling personal data understands that they are contractually responsible for following good data protection practice and failure to do so may lead to disciplinary investigation.
- everyone managing and handling personal data is appropriately trained to do so;
- everyone managing and handling personal data is appropriately supervised;
- anybody receiving and acting on enquiries about personal data knows what to do;
- queries about handling personal data are promptly and courteously dealt with;
- methods of handling personal data are clearly described;
- whenever personal data is transferred outside the European Economic area the College will take steps to establish that all data transferred is appropriate and secure.

Responsibilities

Everyone who works for or with Halesowen College has some responsibility for ensuring data is collected, stored and handled appropriately. Staff must ensure that personal data is handled and processed in accordance with this policy, procedures and the Data Protection Principles.

Data Protection Officer

The Data Protection Officer is the CIS Manager who in liaison with the Director of Finance and Corporate Services will:

- advise the College on its responsibilities, risks and issues
- be responsible for recommending staff training and delivering sessions
- review all data protection procedures and related policies
- liaise with the Information Commissioner as required
- deal with requests from individuals to see data Halesowen College holds about them
- check and approve any contracts with third parties who may handle Halesowen College data

- **CIS and Infrastructure Director**

The CIS and Infrastructure Director is responsible for:

- ensuring all systems, services and equipment used for storing data meet acceptable security standards
- make certain that security hardware and software is functioning properly
- evaluate third party services to store or process data, for example cloud computing

Fair Processing

The Act is not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual to whom the personal data relates.

- The College will ensure that the individual is told:
- that the College is the data controller;
- that the Data Protection Officer is the College's representative;
- the purpose for which the individual's personal data is to be processed by the College; and
- the identity of anyone to whom the personal data may be disclosed or transferred.

The College will ensure that:

- any requirements regarding the consent of an individual of the processing of their personal data have been met. Where information that is regarded as sensitive personal data is processed, explicit consent will usually be required;
- there is legitimate reason for collecting and using all/any personal data collected;
- personal data is not used in any way which has an unjustified adverse effect on individuals;
- it is open and honest about what is collected and how it is used;
- data is handled in ways in which an individual would reasonably expect;
- the data is not used for any unlawful purpose;
- data is kept for a reasonable period. The length of this retention period depends on the purpose for which it was obtained and its nature. It may be necessary to keep data for a reason set out in Schedules 2 and 3 of the Act.

When collecting personal data an oral or written privacy notice should be issued which states simply the identity of who is collecting data and the purpose(s) for which it will be processed.

Data Security Breach

In the event of a reported data security breach leading to the accidental or unlawful destruction, loss, alteration authorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, the College will make every effort to inform affected individuals as appropriate and will liaise with the Information Commissioner to the extent required.

Review

Reviewed/Approved	By	Date
Updated by	Jacquie Carman	23.09.16
Approved at	CE	28.09.16

Data Protection Procedures

Introduction

Halesowen College has a Data Protection Policy reference 01-0015

Relevant Legislation includes

- Data Protection Act 1998 (the "Act")
- EC Directive 95/46/EC
- Freedom of Information Act 2000
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Data Protection is a complex area and therefore it is important to adopt a common sense approach. The following is a guide on the Act and its definitions plus a practical guide on the responsibilities of staff regarding data protection.

Note that in May 2018 the General Data Protection Regulation (GDPR) will come into force. This is European Legislation so it depends on timescales for the UK to leave the European Community whether the GDPR will apply in the UK. If it does or similar UK law is introduced, the five key changes are:

- a broader definition of personal data including IP addresses and cookies;
- new definition of consent; freely given, informed, specific and unambiguous;
- notify breaches within 72 hours;
- increased sanction to 4% of turnover;
- increased information requirements of six data principles.

Useful Contacts

Assistance regarding Data Protection issues can be obtained within College from the following staff:

- Ruth Broome, CIS Manager, ext 7634
- Jacquie Carman, Director of Finance and Corporate Services, ext 7648
- Penny Mitson, Skills and Performance Director, ext 7682
- Jonathan Priest, CIS and Infrastructure Director, ext 7834
- Julia Stevens, Organisational Development Director, ext 7612
- Lynn Pass, Safeguarding and Inclusion Manager, ext 7760

The Information Commissioner

The Information Commissioner is the UK's independent authority who upholds information rights in the public interest, promoting openness and data privacy for individuals.

The Act makes the Information Commissioner responsible for:

- promoting good practice
- issuing advice

- maintaining a register
- resolution of disputes

The Information Commissioner has powers to conduct an audit of the College's systems with the consent of the College. Any requests for assessment or audit must be passed immediately to Director of Finance and Corporate Services.

Following any complaint the Information Commissioner may issue an enforcement or information notice. These must be referred immediately to the Director of Finance and Corporate Services who will notify the Principal and ensure a suitable response is provided within the timescales. Also any changes to systems, correction to inaccurate data etc will be coordinated by the Director of Finance and Corporate Services. Failure to comply with a notice is a criminal offence.

A useful website is www.ico.gov.uk

The Information Commissioner's helpline is 01625 545 745.

The Data Protection Act

The aim of the legislation is to balance the rights of individuals with respect to the processing of personal data with the ability for organisations to operate effectively.

Key definitions contained in the Act and used in the College's Data Protection Procedures include the following:

- Personal data means data relating to a living individual who can be identified from that data (or from data and other information in the College's possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). The scope of what can be regarded as personal data is very wide ranging and covers information held on computer or other media, or on paper within a relevant filing system. Examples of information that may be personal data include:

- CCTV images (please refer to specific guidance regarding data protection and CCTV, including the College's Code of Practice, at Appendix 3 to these Procedures)

- Photographs (please refer to specific guidance regarding data protection and photographs at Appendix 6 to these Procedures)

- Factual information about a person

- Statements of opinion about a person

- The definition of a relevant filing system is any set of information relating to individuals which is structured in such a way that information relating to a particular individual is readily accessible.

- Sensitive personal data means personal data consisting of information about:
  - race/ethnicity
  - political opinions and trade union membership
  - religious or similar beliefs
  - physical or mental health
  - sexuality
  - criminal allegations offences convictions and sentences

Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

- Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

- Photographs meet the definition of personal data when individuals can be easily identified. Certain group shots or photographs taken at a distance may not, as no-one can be picked out.

Data Protection Principles

The Act includes eight basic principles which are included in full as an Appendix 1 to these Procedures.

In summary the principles aim to ensure that data is processed fairly and for the purpose for which it was intended. Data collected should not be excessive and must be accurate and up to date. Data should be retained for an appropriate period and measures must be taken to safeguard information against authorised use.

All staff must ensure that they adhere to the Data Protection Principles when collecting, processing and storing personal data. Practical advice on the Data Protection Principles is provided at Appendix 2 to these Procedures.

The Rights of Individuals

Everyone has a right to know what personal data about them is being held and processed and to whom such personal data may be disclosed. An individual has the following rights (right to subject access) under the Act:

- a right of access to a copy of the information comprised in their personal data;
- a right to object to processing that is likely to cause or is causing damage or distress;
- a right to prevent processing for direct marketing;
- a right to object to decisions being taken by automated means;
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to claim compensation for damages caused by a breach of the Act.

Therefore it is very important to have a simple Data Protection statement included on key documents, for example the student learning agreement.

Under the right of subject access above, an individual is entitled only to their own personal data and not to information relating to others. The College does not usually have to comply with a disclosure request to provide information relating to the individual making the request and another individual unless the other individual has consented to disclosure.

However it is permitted in certain circumstance to disclose information to a third party without telling the individual if it is to meet a legal obligation for example CSA requests for salary details, or HM Revenue and Customs inspectors. These are:

- the prevention or detection of crime;

- capture or prosecution of offenders; and
- the assessment or collection of tax/duty

Refer to Appendix 5 – Releasing Information to Prevent or Detect Crime.

As stated above, individuals have a right to subject access. Individuals may make a written request (including email and facsimile) to the College (a "subject access request"). Under the Equality Act 2010 the College will make reasonable adjustment and accept a verbal request from an individual with a disability, learning difficulty, medical condition or limited written skills who finds it unreasonably difficult to make a request in writing. Requests must be made to the Data Protection Officer. The request will be dealt with as soon as the individual pays the appropriate fee. The individual is usually entitled to be given details of the data held, the purpose for which it is being processed and to whom it may be disclosed. Hence the individual has a right to a copy of all the personal data held about them irrespective of when the records were created. Before the request is actioned the College must be certain that the person making the request is the individual about whom the personal data relates. Also, the College is allowed to ask for any information reasonably required to find the personal data covered by a request. It is vital that the College has a central record of where all data is held so that it can comply with requests for information and comply with the Act. Requests for information must be actioned as soon as possible and always within 40 days.

The right to subject access is subject to certain exemptions specified in the Act. These include, for example:

- exemptions from disclosure of confidential references, examination marks and examination scripts; and
- a provision that there is no need to comply with a request if it is similar or identical to one complied with earlier unless a reasonable interval has elapsed.

The Information Commissioner has published various practice notes on these exemptions.

Charges

The College may charge an individual a fee for responding to a subject access request. The maximum fee chargeable is generally £10 per subject access request although there are special rules applicable to education records where a sliding scale from £1 to £50 applies depending on the number of pages provided. No VAT should be charged as subject access requests are outside the scope of VAT.

Disclosure of Information to Third Parties (also refer to Appendix 5)

Information about an individual should not be disclosed to an appropriate third party unless

- the individual has given consent;
- applicable under the provisions of the Mental Capacity Act 2005;
- there is a real risk of harm to a child hence the safeguarding of a child's welfare overrides the need to keep the information confidential – any matters of this nature must be referred to the College nominated safeguarding officers without delay.

Where a third party, eg a solicitor is acting on behalf of an individual, written authority from the individual concerned must be requested before the request is processed.

Requests made by parents and guardians for data about children/young people are subject to the Act. The data is about the individual and does not belong to a parent/guardian. The following considerations must be applied:

- the child's level of maturity and their ability to make decisions;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Usually for students at Halesowen College personal data should not be disclosed to a parent/guardian unless the student has consented to information being shared with that person in their learning agreement. Any issues or concerns must be discussed with the Safeguarding and Inclusion Manager.

In the event that the College becomes the data controller in respect of personal data collected from a child, this personal data may not be disclosed or transferred to third parties without the explicit and verifiable consent of the child's parent or guardian, unless it is clear that the child understands the implications of his or her actions.

As stated above there are exemptions when information must be disclosed to a third party. Exemptions do not require the College to automatically disclose personal data to the police or other law enforcement agencies – they merely ensure the parameters of the Act are not breached (see Appendix 5).

Possible Sources of Data Covered by the Act

- HR/payroll files and records including HMRC records
- Student files and individual learning plans; student data held on STARS
- Email messages and documents/memos/letters
- Enrolment forms/learning agreements
- Registers and Curriculum Record Books
- Student visit records
- Financial records for example invoices
- Expenses claims
- Photograph and video images
- Social media posts

Possible Location of Data Covered by the Act

- Formal files
- Central filing systems
- Ad hoc files held by managers/team leaders

- Files in storage/archive
- Information held by third parties eg payroll bureau
- Notebooks
- CCTV archived images
- Computerised systems operating both centrally and locally

Responsibilities of Staff

- Staff should not share data informally. When access to confidential information is required, staff can request it from their line managers.
- Halesowen College will provide training to all employees to help them understand their responsibilities when handling data; it is the responsibility of staff to attend such training.
- Staff should keep all data secure, by taking sensible precautions and following the guidelines.
- Strong passwords must be used and they must never be shared.
- Personal data should not be disclosed to unauthorised people, either within the College or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Staff should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Appendices

Appendix 1 Data Protection Principles

Appendix 2 Practical Advice on Data Protection Principles

Appendix 3 Data Protection and CCTV

Appendix 4 Data Security Summary Guidelines

Appendix 5 Releasing Information to Prevent or Detect Crime

Appendix 6 Use of Photographs/Images

The Data Protection Principles

First Principle

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

- At least one of the conditions in Schedule 2 of the Act (see below) is met; and
- In the case of sensitive personal data, at least one of the conditions in schedule 3 of the Act (see below) is also met

Second Principle

Personal data can only be obtained for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

Third Principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.

Fourth Principle

Personal data shall be accurate and, where necessary, kept up to date.

Fifth Principle

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or purposes.

Sixth Principle

Personal data shall be processed in accordance with the rights of data subjects under the Act.

Seventh Principle

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Eighth Principle

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level or protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Conditions applicable under Schedule 2 of the Act

1. The individual to whom the personal data relates has given his/her consent to the processing.

2. The processing is necessary:

   - for the performance of a contract to which the individual to whom the personal data relates is a party, or
   - for the taking of steps at the request of the individual to whom the personal data relates with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the College is subject, other than an obligation imposed by contract.

4. The processing is necessary in order to protect the vital interests of the individual to whom the personal data relates.

5. The processing is necessary:

   - for the administration of justice;
   - for the exercise of any functions of either House of Parliament;
   - for the exercise of any functions conferred on any person by or under any enactment;
   - for the exercise of any functions of the Crown, a Minister of the Crown or a government department; or
   - for the exercise of any other functions of a public nature exercised in the public interest by any person.

6. The processing is necessary for the purposes of legitimate interests pursued by the College or by the third parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the individual to whom the personal data relates.

   The relevant Secretary of State may by order specify particular circumstances in which this condition 6 is, or is not, to be taken to be satisfied.

Conditions applicable under Schedule 3 of the Act

1. The individual to whom the personal data relates has given his/her explicit consent to the processing of the personal data.

2. The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the College in connection with employment.

   The relevant Secretary of State may by order:

   - exclude the application of sub-paragraph (1) in such cases as may be specified, or

- provided that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary:

- in order to protect the vital interests of the individual to whom the personal data relates or another person, in a case where:
  - consent cannot be given by or on behalf of the individual to whom the personal data relates, or
  - the College cannot reasonably be expected to obtain the consent of the individual to whom the personal data relates, or
- in order to protect the vital interests of another person, in a case where consent by or on behalf of the individual to whom the personal data relates has been unreasonably withheld.

4. The processing :

- is carried out in the course of its legitimate activities by anybody or association which –
  - is not established or conducted for profit, and
  - exists for political, philosophical religious or trade-union purposes;
- is carried out with appropriate safeguards for the rights and freedoms of data subjects,
- relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes; and
- does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the individual to whom the personal data relates.

6. The processing:

- is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
- is necessary for the purpose of obtaining legal advice, or
- is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. The processing is necessary:

- for the administration of justice,
  - for the exercise of any functions or either House of Parliament,
- for the exercise of any functions conferred on any person by or under an enactment, or

- for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

- The relevant Secretary of State may by order:
  - exclude the application of sub-paragraph (1) in such cases as may be specified, or
  - provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

- The processing:
  - is either:
    - the disclosure of sensitive data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or
    - any other processing by that person or another person of sensitive personal data so disclosed; and
    - is necessary for the purposes of preventing fraud or a particular kind of fraud.
- In this paragraph “anti-fraud organisation” means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes.

8. The processing is necessary for medical purposes and is undertaken by:
   - a health professional, or
   - a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

- In this paragraph “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. The processing:
   - is of sensitive personal data consisting of information as to racial or ethnic origin,
   - is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

- is carried out with appropriate safeguards for the rights and freedoms of individuals to whom personal data relates.

- The relevant Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of individual to whom the personal data relates.

10. The personal data are processed in circumstances specified in an order made by the relevant Secretary of State for the purposes of this paragraph.

Practical Advice on the Data Protection Principles

1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

- At least one of the conditions in Schedule 2 of the Act is met; and
- In the case of sensitive personal data, at least one of the conditions in schedule 3 of the Act is also met

In practice, it means that you must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure you do not do anything unlawful with the data.

2 Personal data can only be obtained for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes

In practice, the second data protection principle means that you must:

- be clear from the outset about why you are collecting personal data and what you intend to do with it;
- comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;
- comply with what the Act says about notifying the Information Commissioner; and
- ensure that if you wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed

In practice, it means you should ensure that:

- you hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual; and
- you do not hold more information than you need for that purpose.

4 Personal data shall be accurate and, where necessary, kept up to date

To comply with these provisions you should:

- take reasonable steps to ensure the accuracy of any personal data you obtain;
- ensure that the source of any personal data is clear;
- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to update the information.

5 Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or purposes

In practice, it means that you will need to:

- review the length of time you keep personal data;
- consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date.

6 Personal data shall be processed in accordance with the rights of data subjects under the Act

This is the sixth data protection principle, and the rights of individuals that it refers to are:

- a right of access to a copy of the information comprised in their personal data;
- a right to object to processing that is likely to cause or is causing damage or distress;
- a right to prevent processing for direct marketing;
- a right to object to decisions being taken by automated means;
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to claim compensation for damages caused by a breach of the Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

In practice, it means the College must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised with which you must comply. In particular, the College will need to:

- design and organise its security to fit the nature of the personal data you hold and the harm that may result from a security breach;
- be clear about who in the College's organisation is responsible for ensuring information security;

- make sure the College has the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively.

(Refer to Halesowen College Data Security Guidelines)

8 Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level or protection for the rights and freedoms of data subjects in relation to the processing of personal data

Putting personal data on a website will often result in transfers to countries outside the EEA. The transfers will take place when someone outside the EEA accesses the website. If you load information onto a server based in the UK so that it can be accessed through a website, you should consider the likelihood that a transfer may take place and whether that would be fair for the individuals concerned. If you intend information on the website to be accessed outside the EEA, then this is a transfer.

Data Protection and CCTV

Introduction

Closed circuit television (CCTV) operational in College will inevitably involve the recording of staff, students and members of the public. This is personal data which is subject to the terms and conditions of the Act. Moreover, the Information Commissioner issued a revised CCTV Code of Practice in 2008 which must also be adhered to.

Purpose of CCTV

The purposes for which data (images) are being processed include:

- Public, staff and student safety
- Discipline and security of premises
- Prevention and detection of crime
- Apprehension and prosecution of criminal offenders
- Incident monitoring

This is included in the College's Data Protection Registration.

Operators of the equipment must only use the CCTV to achieve the purposes for which it has been installed.

Code of Practice

Positioning of Cameras and Information

- The College shall display notices which are clearly visible and legible informing staff, students and members of the public that CCTV is in operation inside the building or in the immediate vicinity of the area under surveillance. These signs must state that Halesowen College is responsible for CCTV, the purpose of the scheme and the contact details of the data controller.
- Only in an exceptional circumstance, for example when criminal activity is identified and evidence needs to be collected, would CCTV be operational without notice. This must be documented and an assessment made as to whether the use of signs would prejudice successfully obtaining the evidence. Monitoring should only be for as long as necessary.
- The cameras must be situated so that they only monitor those areas which the College intends to monitor. Operators of the equipment should not be able to alter the areas/range of areas covered to examine other areas outside the College which compromise privacy.
- The images recorded may be either constant real-time or periodic planned monitoring.
- Any camera used to protect an ATM machine and individuals using the facility and/or an area where chip and pin payments are taken, must not capture images of pin numbers or balance enquiries.

Quality of Image

- Images produced by the CCTV should be as clear as possible in order that it is effective for the intended purposes.
- Regular checks should be performed by the IT Services Technicians to ensure that the system is working properly.
- A maintenance and service log of the CCTV system should be maintained by the Estates Manager.
- Where the CCTV images are recorded on tape or similar then these should be of good quality and cease to be used when the quality of image deteriorates. The medium should be cleaned so that images are not recorded on top of images previously recorded.

Retention of Images

- Images should only be kept for as long as necessary. As a general rule, images shall be kept for between 7 and 14 days unless required for a specific purpose.
- Once the retention period has expired the images will be erased by an automatic overwrite. As part of the regular checks, the technician will check to ensure such deletion is permanent.
- Any retained images, relating to an alleged or actual incident, should be kept in a secure location [either a physical location (block 2 downstairs safe) or within the CCTV recorder]. The date of the images and any crime number should be noted. Removal or erasure of these images must be authorised by the Principal, however images will not be kept any longer than strictly necessary to meet the purpose for retaining them.

Viewing of Images

- Access to and disclosure of images recorded by CCTV must be restricted and carefully controlled to protect the rights of individuals and to ensure any evidence remains intact.
- CCTV footage can be viewed in real-time by the receptionist, duty managers, College Executive/SMT, Estates Manager, CIS and Infrastructure Director, Network Manager, caretakers, security personnel and technicians for the purposes specified above and/or routine maintenance of the system.
- Viewing of real time images can be viewed where there are access points. The retrospective viewing of recorded images should only take place in designated areas (offices and other non-public areas).
- Retrospective viewing of images in order to collate evidence relating to an alleged incident is permissible on the authority of a CE/SMT member*, HR Adviser or Estates Manager. The purpose of the request must be logged and the CCTV request form completed.
- Those filmed may wish to view the CCTV at a certain date/time and can make a Data Protection request to see this footage. This can be arranged provided that it does not infringe the data protection or privacy rights of others. A fee of £10 is chargeable and a response must be provided within 40 days. Requests shall be processed in accordance with the main Data Protection Policy. It is important to ensure that images of other people are not disclosed in responding to a subject access request. Images of others should

*The Student Experience Director must be notified (whenever possible) whenever the alleged incident involves students.

therefore be disguised or blurred if this is technically possible. The CCTV request form should be completed. Access may only be denied when the images to which the data subject has requested access are held for the prevention or detection of crime and/or apprehension of offenders or may put an individual at risk.

- The College may disclose CCTV images to the following:

  - security organisations
  - business associates and professional advisers
  - persons making a data protection enquiry (subject to relevant restrictions)
  - police

  for the purposes defined above. Again a CCTV request form should be completed and authorised appropriately. A copy of every completed CCTV form must be filed with the Data Co-ordinator. Removal of images from the premises of Halesowen College must be documented as follows:

  - date and time of removal
  - name of person removing the images
  - name of person viewing the images
  - reason for removal and viewing
  - date and time of return

Standards

- All staff should be aware of the restrictions
- Access to images should be recorded
- Disclosure of recorded images should be limited and in prescribed circumstances

Halesowen College

CCTV Request Form

Name of person requesting footage	
Staff member of Halesowen College	❑ Yes ❑ No
Data subject (£10 charge)	❑ Yes ❑ No
Third party (including police)	❑ Yes ❑ No
Please specify name and contact details	
Reason for request	
Date of image	
Data subject(s) in image	
Crime no. (if applicable)	
Access authorised by	
If access denied please state reason	
Images shown by	Date Time
Further action (if any)	
Image on disk supplied	❑ Yes ❑ No
Disk received by	
Signed	
Date	
Date returned	
Received in College by	

Data Security Summary Guidelines

In accordance with the seventh data principle it is important to ensure security of data and protect information against loss, damage or destruction. This document is a summary of best practice guidelines for data security.

Usernames and Passwords

Your username and password are the first line of defence for most of the systems you have access to.

- You must use non obvious strong passwords; random mix of a minimum of six alpha (mixed case) and at least one numeric plus a special character is required;
- Change your password regularly (mandatory once every half term) and for system administrators this will be required every 30 days);
- Do not write your password down;
- Do not share your password with others.

Storing and Using Data

When data is in electronic format it must be protected from unauthorised access, accidental deletion and hacking.

- Do not store data on portable drives or removable media. If there is no alternative then encryption must be used and all removable media should be kept locked away securely when not being used.
- Use the most appropriate drive/system to store your data. Remember some drives are accessible to everyone including students. Seek advice if you are unsure.
- When working with personal data, lock screens when away from your desk.
- Store data on designated network drives, not PC local disks, laptops or tablets.
- Data must only be uploaded to approved cloud computing services.
- Access data directly from the College network wherever possible (remote facilities are available) – do not make unnecessary copies of files.
- Be cautious about emailing data, as the message can easily be forwarded to others. Sensitive data should be encrypted before being transferred electronically.
- Do not publish any personal, confidential, sensitive or inappropriate data on a social media site.

When data is stored on paper.

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Paper prints should not be made unless necessary and not left where unauthorised people could see them, eg a printer.
- Printouts should be disposed of securely when no longer required.

Data Accuracy

The law requires Halesowen College to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that personal data is accurate, the greater the effort Halesowen College should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a student's details when there is an opportunity to do so.
- The College will make it easy for data subjects to update the information held about them.
- Data should be updated as inaccuracies are discovered. For instance, if a student can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the Student Experience Director's responsibility to ensure marketing databases are checked against industry suppression files at least every six months.

General Points

- Use data only for the purpose for which it is provided.
- The only people able to access data covered by this policy are those who need it for their work.
- If you feel you have an inappropriate level of access to any system you should notify your line manager.
- Data should not be shared informally nor disclosed to unauthorised people either within the College or externally.
- Notify your line manager immediately if there is a suspected breach of security, no matter how insignificant it may seem.

Releasing Information to Prevent or Detect Crime

There is an exemption in the Act that allows the College to give out personal data because it is needed to prevent or detect a crime, or catch and prosecute a suspect (Section 29 – Crime and Taxation). There are, however, limits on this exemption and what can be released.

The police are most likely to ask the College to release personal data under this exemption. However, requests may be received from other organisations that can rely upon this exemption because they have a crime prevention or law enforcement function, for example, the Department for Work and Pensions – Benefits Fraud Section or release of information relating to the College's Prevent duty as specified by the Counter Terrorism and Security Act 2015.

As stated above, the exemption does not cover the disclosure of all personal data, in all circumstances. It only allows the release of personal data for the stated purposes and only if not releasing it would be likely to prejudice/significantly harm any attempt by police to prevent crime or catch a suspect.

For every request for personal data received (and about each separate individual), the following questions must be asked:

- Is the person making the request who they say they are? For this reason particular care should be taken over the telephone and in such situations a data protection facsimile or email must be requested and received before the request can be actioned.
- Is the person asking for this information doing so to prevent or detect a crime or catch or prosecute an offender?
- If the personal data is not released will this significantly harm any attempt by the police to prevent crime or catch a suspect?

There are times when it may be necessary to release personal data relating to more than one person who the police do not name, but who fit a particular description.

In such instances it is important to be satisfied that the police have narrowed the description of the suspect as much as they reasonably can.

If it is deemed unreasonable to provide information then ultimately the police can come back with a court order requiring the release of the personal data. If the court decides the information should be released the College would not be in breach of the Act by obeying the order.

The Director of Finance and Corporate Services is responsible for the release of information to a third party. A request may be authorised by the Director of Finance and Corporate Services or the Safeguarding and Inclusion Manager. However, the Principal must authorise the release of personal data under the exemption which relates to a member of staff.

All requests must be made in writing (facsimile/email) and signed by someone of sufficient authority.

A record must be made of each decision taken and the reasons why a particular decision was made. These records will be maintained by the Director of Finance and Corporate Services.

Use of Photographs

The Data Protection Act 1998 regulates the use of all personal data including photographs from, which people can be identified, and recordings.

The College uses images in its marketing material and must gain permission from individuals being photographed and/or videoed. This permission must be in place before any photographs are taken.

The College will provide clear information about what the pictures will be used for and once a photograph/video has been taken it must only be used for the purpose(s) indicated.

The College learning agreement states that the College may use images/photographs in marketing materials. Students have the option to object by contacting the Data Co-ordinator in writing. Moreover, staff, students and external visitors etc should sign a consent form.

Images may be used on the College website. The Act provides specific rules for the transfer of information outside the European Union. The Halesowen College website can be viewed worldwide hence 'active' permission is needed to use images. This permission must be clear and recorded; verbal consent is not adequate.

It is good practice not to use the names of children (under 16) if their photographs appear on websites even when consent is in place.

Parental consent for the use of photographs etc is only required for young people under age 16.

Halesowen College

Student Photography Approval Form

Full name (capitals) _____

Age _____

Course _____

Former secondary school _____

Date _____

Photocall details
(event, publicity) _____

I consent to allow Halesowen College and approved organisations to use the photograph(s) of the above named person in publicity material to promote the work of Halesowen College. It will not be used for any other purpose. The photographs may be used for publicity including websites, display and print.

I may write at any time to the address below to withdraw consent, providing such information as is necessary to identify the photos, in order that they may be withdrawn from the library and not used in any further publicity material.

Signature _____

Gill James
Halesowen College
Whittingham Road
Halesowen
West Midlands
B63 3NA

Halesowen College

Staff Visitor Photography Approval Form

Full name (capitals) _____

Title _____

Organisation _____

Former secondary school _____

Date _____

Photocall details
(event, publicity) _____

I consent to allow Halesowen College and approved organisations to use the photograph(s) of the above named person in publicity material to promote the work of Halesowen College. It will not be used for any other purpose. The photographs may be used for publicity including websites, display and print.

I may write at any time to the address below to withdraw consent, providing such information as is necessary to identify the photos, in order that they may be withdrawn from the library and not used in any further publicity material.

Signature _____

Gill James
Halesowen College
Whittingham Road
Halesowen
West Midlands
B63 3NA