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. The use of personal data by Halesowen College is regulated by the General Data Protection Regulation (the GDPR), which replaces the Data Protection Act 1998 (DPA) on 25 May 2018.

Personal data

Any information, whether deemed confidential or not, relating to an identified or identifiable living individual is personal data. An identifiable person is one who can be identified directly or indirectly. Personal data may be factual (such as name, address or date of birth) but it does not need to include a person's name to amount to personal data. It also includes opinions and judgments about individuals (such as a performance appraisal). Personal data also includes special categories of data (which was referred to as "sensitive" personal data under the DPA. The special categories are personal data relating to racial or ethnic origin, political opinions, religious/philosophical beliefs, trade union membership and the processing of (using) genetic data, biometric data or data concerning a person's health, sex life or sexual orientation ("sensitive personal data").

The term "personal data" is used in this policy to denote both sensitive and non-sensitive personal data unless otherwise specified.

Personal data relating to criminal offences and convictions is dealt with separately by the GDPR and is required to be processed only under the control of "official authority" or when authorised by UK law. i.e. in accordance with the law relating to the rehabilitation of offenders and with the Disclosure and Barring Service's scheme.

An individual whose personal data is being processed by the College is a known as a "data subject".

Processing

The GDPR regulates the "processing" of personal data. Processing refers to anything that can be done to personal data from its creation to its destruction, including both creating and destroying personal data.

This policy describes how personal data must be processed (e.g. collected, handled and stored) in a way that ensures:

- compliance with the law and best practice
- protection of the rights of individuals
- openness about processing of personal data
- avoidance of risk of a data breach
- obligation to provide comprehensive, clear and transparent privacy policies
- adequate internal records of processing activities

The lawful and proper processing of personal data by Halesowen College is very important to successful operations, and in maintaining confidence with those with whom the College interacts. Halesowen College therefore ensures personal data is processed in accordance with the principles of data protection as set out below. The GDPR confers a number of rights on data subjects, which are also listed below.

The College, including all members of staff must comply with the GDPR and this policy in relation to all personal data it processes and stores electronically and in relation to some physical records.

All staff were asked to attend a training session on the new requirements for GDPR when it was introduced and since then new staff use EduCare package

The Data Principles

The College recognises that failure to hold and process information in a fair and proper way breaches the privacy of those whose personal data is entrusted to it and could. In appropriate circumstances some breaches may amount to a criminal offence.

Specifically, the new Principles require that personal data:

i processed lawfully, fairly and in a transparent manner in relation to individuals;

ii collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

iii adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

iv accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

v kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

vi processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

The College is required to implement technical and College-wide measures to ensure that the principles are implemented effectively (“privacy by design and default” – see section on Data Protection Procedures).

Lawful Processing

In order to process personal data, the College has identified and documented the legal basis for doing so. In order to be lawful, the College must comply with one of the following conditions for processing:

- Consent of the data subject
- Processing is necessary for the performance of a contract with the data subject or to take

steps to enter into a contract

- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of a data subject or another person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (*This condition is not available to "public authorities in the performance of their task and as such the College cannot rely on this condition.)*

Consent is not the only condition and other grounds of justification can be relied on. Consent should usually only be relied on where there is no other available justification. Where the College is, however, relying on the consent of the data subject, then the College must be able to demonstrate that it was freely given, specific, informed and unambiguous for each purpose for which the personal data is being processed i.e. the data subject must have a genuine choice. Consent can be given by a written, including electronic, or oral statement. This could include the data subject ticking a box when visiting a website, choosing technical settings for social network accounts or by any other statement or conduct which clearly indicates their acceptance of the proposed processing of personal data. Silence, pre-ticked boxes or inactivity will not constitute consent. Safeguarding can override data protection if the child's life may be in danger.

When processing sensitive personal data, the College must, in addition to complying with one of the conditions outlined above, comply with one of set of conditions specifically relating to sensitive personal. They include:

- Explicit consent of the data subject.
- The processing is necessary for the purposes of carrying out obligations and exercising rights in the context of employment.
- To protect the data subject's vital interests or another's where the data subject is physically or legally incapable of giving consent.
- Information manifestly made public by the data subject.
- Processing necessary for legal proceedings.
- Substantial public interest subject to proportionality and safeguards for the individual.
- Processing necessary for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes.
- Consent from staff will be gained at the time of applying for jobs and again when contracts of employment are issued and with a Privacy Notice.
- Consent from students will be gained at the point of application.

Rights of data subjects

- A right of access to personal data which the College is processing together with information about the purposes of processing, recipients or categories of recipients, retention periods, and the remaining rights of the data subject.
- A right to rectification of inaccurate personal data and the right to have incomplete personal data completed
- A right to erasure. This is a limited right.
- A right to restrict processing in certain limited circumstances.
- A right to portability of personal data.

- A right to object to processing e.g. for marketing purposes and in other limited circumstances.
- Rights in relation to decisions made solely on the basis of an automated process, including profiling, which has significant consequences for a data subject.

In addition, Halesowen College will ensure that:

- everyone managing, handling and processing 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, handling and processing personal data is appropriately trained to do so;
- everyone managing, handling and processing 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;

Responsibilities

Everyone who works for or with Halesowen College has responsibility for ensuring that personal data is collected, stored and handled and otherwise processed in accordance with this policy, procedures and the GDPR.

Data Protection Officer

The GDPR requires public authorities such as the College to appoint a Data Protection Officer (DPO). The College has designated the Registrar who will:

- advise the College and its employees on its obligation to comply with relevant legislation monitor compliance with the law including managing internal data and advise on data protection impact assessments.
- be responsible for recommending staff training and delivering sessions.
- review all data protection procedures and related policies.
- co-operate and liaise with the Information Commissioner as required.
- have due regard to any risk associated with the College's processing arrangements, taking into account the nature, scope, context and purposes of the College's processing of personal data.
- 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.
- report to the Corporation on data protection issues.

The Information and Director of Information will support the DPO and 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.

Transparency, fairness and accountability.

The law does not prevent the processing of personal data but ensures that it is done fairly/transparently and without adversely affecting the rights of the individual to whom the personal data relates. It also requires that data subjects are provided with certain information in the form of a privacy statement when their personal data is collected, as set out below. The College will ensure that the individual is told:

- that the College is the data controller;
- the contact details of the Data Protection Officer;
- the purposes for which the data subject's personal data is to be processed by the College;
- the legal bases for processing personal data
- where processing is based on legitimate interests, the legitimate interest being pursued
- the recipients or categories of recipient of the personal data
- any transfers of personal data outside of the EEA and adequacy of safeguards.
- the intended retention period and any clauses affecting it
- the data subjects' rights
- where processing is based on consent, the right to withdraw that consent at any time
- the right to submit a complaint to the Information Commissioner
- where the personal data is needed in order to perform a contract or to enter into it, or to fulfil a statutory obligation, the possible consequences of not providing it
- the existence of any automated decision making or analytical processing.
- the purposes for which the personal data will be processed in addition to the purposes for which it was obtained.

Where personal data is obtained from someone other than the data subject (i.e. a third party) additional information must be provided as follows:

- The categories of personal data
- The source of the personal data

There are some exemptions from this requirement.

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 will be rectified where an error is identified
- 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.

When collecting personal data, a written privacy notice will be issued in accordance with the GDPR requirements outlined above.

Data Security Breach

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

It is important for the College to take all reasonable steps to prevent breaches occurring and to address promptly any breaches that do occur. Serious breaches, if unaddressed, may have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, identity fraud, financial loss, loss of confidentiality, distress or any other significant economic or social disadvantage.

The College is required to notify the Information Commissioner of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

This must be assessed on a case by case basis.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the College must notify the data subjects concerned directly, unless the College had taken steps to render the personal data unintelligible or has taken subsequent steps to remove the risk. Where notifying the data subjects directly would involve disproportionate effort, the College may instead make a public or similar announcement which is equally effective in informing the data subjects.

The threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

What information must a breach notification contain?

- The nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- The name and contact details of the data protection officer or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken by the College, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the College becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.

Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2 per cent of turnover.

Code of Practice

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

- comply with the conditions regarding the collection and use of information 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 ensuring all necessary corrective action is taken expediently;

- apply strict checks to determine the length of time information including images is held and to comply with the retention periods so determined;
- ensure that the rights of people about whom information is held can be exercised under the law;
- take appropriate technical and organisational security measures to safeguard personal data;
- ensure that personal data is not transferred outside the EEA unless the relevant condition provided for in the GDPR is complied with by the College, e.g. where the country is listed by the EU Commission as having adequate protection, the transfer is subject to standard contractual clauses approved by the EU Commission, the transfer is subject to the explicit consent of the data subject (this is not an exhaustive list);
- observe and understand derogations in the GDPR

Reviewed/Approved	By	Date
Updated by	Jacquie Carman	17.11.2021
Approved at	CLT	29.11.2021
Approved at	Corporation	30.11.2021
Date of Next Review		01.11.2022
Website	Yes / No	Yes

Data Protection Procedures

Introduction

The College is required to implement appropriate technical and organisational procedures to ensure that the data-protection principles are implemented effectively (data protection by design a default).

Data Protection is a complex area and therefore it is important to adopt a common sense approach. The following is a guide on the regulation and its definitions plus a practical guide on the responsibilities of staff regarding data protection.
From 25 May 2018 the General Data Protection Regulation (GDPR) will come into force. 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 sanctions; (up to 20 million Euros)
- data protection principles which are similar to the existing principles under the DPA.

Useful Contacts

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

- Jacquie Carman, Vice Principal/Chief Operating Officer, ext 7648
- Ruth Broome, Registrar, ext 7634
- Rachael Charles HR Business Partner ext 7814
- Kate Masters Personnel Manager ext 7614
- Jonathan Priest, Director of Information Services, ext 7834
- Lynn Pass, Designated Safeguarding Lead, ext 7760

Support can also be sought from members of the GDPR Steering Group who regularly meet provide strategic direction and leadership to ensure that Halesowen College is as compliant as practically possible with the General Data Protection Regulations (see Appendix 7).

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 the Chief Operating Officer/ Vice Principal. There is a requirement for privacy impact assessments in some circumstances under the GDPR e.g. where there is large scale processing of personal data relating to criminal convictions.

Complaints about the College's processing of personal data can be referred to the Information Commissioner.

Following any complaint, the Information Commissioner may issue an enforcement or information notice. These must be referred immediately to the Chief Operating Officer/ Vice Principal 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 Chief Operating Officer/ Vice Principal. Failure to comply with a notice is a criminal offence.

A useful website is https://ico.gov.uk

The Information Commissioner's helpline is 0303 123 11130.

Examples of Personal Data

- Examples of information that may be personal data as defined in this policy 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
- Data contained in manual records that are a ""filing system" which is defined as "any structured set of personal data which are accessible according to specific criteria, whether centralise, de-centralised or dispersed on a functional or geographic basis" In essence this means any manual record which is structured to enable specific information about individuals to be readily accessible.
- Sensitive personal data (see definition on page 1) will be include:
- Health records
- DBS checks
- Information in equality monitoring forms e.g. details of sexual orientation,
- Details of staff and student disabilities:

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

- 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

All staff must ensure that they adhere to the Data Protection Principles as set out at the beginning of this 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

These rights are set out in detail in this policy. One of the most important rights is to know what personal data about them is being held and processed and to whom such personal data may be disclosed. The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing
It is very important also to have a simple Data Protection statement/privacy 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. Where is it not possible to disclose a data subject's own data without also revealing the personal data of a third party, the third-party data should only be disclosed if it is reasonable in all the circumstances of the particular case to disclose it. Whether the consent of the third party was sought and if so, refused can be taken into account when assessing reasonableness.

However, it is also permitted in certain circumstance voluntarily to disclose information to a third party without telling the individual if it is for the following purposes:

- the prevention or detection of crime;
- apprehension or prosecution of offenders; and
- the assessment or collection of tax/duty

Some government agencies and other bodies have a legal right to require disclosure of information for example Child Support Agency requests for salary details, or regulatory bodies such as the Health Care Professions Council. If a requester is purporting to exercise a specific statutory right to obtain personal data, staff should ask for details of the legislation on which the requester is relying. All such requests will be dealt with by the Data Protection Officer

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

Procedure for subject access requests

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 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 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 one month. This timescale can be extended a further two months where requests are complex or numerous. In such cases the College will inform the individual within one month of the receipt of the request and explain why the extension is necessary. If a request is manifestly unfounded or excessive the request will be refused. Where data is provided electronically it must be in a structure format to enable data portability.

Charges

The College must provide a copy of the information free of charge. However, where a request is manifestly unfounded or excessive, particularly if it is repetitive, a reasonable charge will be levied based on the administrative cost of providing the information. A similar charge will be made for repeat copies for the same information.

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

Information about an individual should not be disclosed to a 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, e.g. 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 GDPR. As a general principle, parents have no automatic right of access to their children's personal; data. 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.

Where the College collects personal data direct 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 for voluntary disclosure to certain third parties. Exemptions do not impose a duty on the College to automatically disclose personal data to the police or other law enforcement agencies – they merely enable disclosure without breaching the GDPR. The disclosures will however need to be justified in each case (i.e. comply with the conditions set out above (see also Appendix 5).

Categories of Personal Data Covered by the Act

- HR/payroll files and records including HMRC records
- Student files and individual learning plans; student data held on My Halesowen
- Details of students' staff members' health and disability
- DBS checks – personal data relating to criminal convictions and alleged offences
- 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 e.g. payroll bureau
- Notebooks
- CCTV archived images
- Computerised systems operating both centrally and locally
- Computerised systems operating remotely within controlled cloud environments
- Third-part computerised systems and services

Responsibilities of Staff

- Staff should not share personal data without justification. Sensitive personal data in particular should only be shared with other members of staff who need to know it (for example in order to make adjustments for individual disabled students). When access to confidential information is required, staff can request it from their line managers. See above for providing personal data to third parties.
- 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 of at least six alpha numeric digits, mixed case and with a special character must be used and they must never be shared.
- 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. The College has a retention of documents policy which can be accessed From http://data.halesowen.ac.uk/reports.
- Staff should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.
- Personal data should not be shared on platforms such as Teams

APPENDICES

Appendix 1 Accountability Principle
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

Appendix 1

Accountability Principle

The accountability principle requires that the College demonstrates compliance with the principles and states explicitly that this is the College's responsibility.

To demonstrate compliance the College

- Implements appropriate technical and organisational measures that ensure and demonstrate compliance including internal data protection policies, staff training, internal audits of processing activities, and reviews of internal HR and other relevant policies.
- Maintain relevant documentation on processing activities.
- Appoint a data protection officer.
- Implement measures that meet the principles of data protection by design and data protection by default including:
    - Data minimisation;
    - Pseudonymisation – minimising the opportunity for individuals to be identified e.g. use of ID codes;
    - Transparency;
    - Allowing individuals to monitor processing;
    - Creating and improving security features on an ongoing basis;
    - Use data protection impact assessments where appropriate.

A DPIA will be conducted when using new technologies; and

- the processing is likely to result in a high risk to the rights and freedoms of individuals.
- Processing that is likely to result in a high risk includes (but is not limited to):
- systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.
- large scale processing of special categories of data or personal data relation to criminal convictions or offences.
- large scale, systematic monitoring of public areas (CCTV).

The DPIA will contain

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that compliance.
- A DPIA can address more than one project.

Appendix 2

Practical Advice on the General Data Protection Principles

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

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, this 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 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)

7 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. Such transfers need to comply with the requirements of the GDPR.

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, revised in 2017, 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 relevant IT Services to ensure that the system is working properly.
- A maintenance and service log of the CCTV system should be maintained by the Estates Manager.

Retention of Images

- Images should only be kept for as long as necessary. As a general rule, images may be kept for between 714 and 21 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 technical staff will ensure that affected materials are deleted and thus unavailable for retrieval.
- Any retained images, relating to an alleged or actual incident, should be kept in a secure location [either a physical location or within the CCTV Management System]. 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, CLT, Head of Estates and Facilities, Network Manager, Operations Director , estates and operations teams, security personnel and authorised 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 College Leadership Team member or Head of Estates and Facilities. 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 request to see this footage. This can be arranged provided that it does not infringe the data protection or privacy rights of others. 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 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

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).
- Only use your credentials to access verified, and approved services.
- 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/cloud 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, e.g. 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 Marketing Manager'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 Chief Operating Officer/ Vice Principal is responsible for the release of information to a third party. A request may be authorised by the Chief Operating Officer/ Vice Principal 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 Chief Operating Officer/ Vice Principal.

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.

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 _____

Helen Burgoyne
Marketing Manager
Halesowen College
Whittingham Road
Halesowen
West Midlands
B63 3NA

Staff Visitor Photography Approval Form

Full name (capitals) _____

Title _____

Organisation _____

Former secondary school _____
(Data collection may need to refined; learners should be able to provide their student ID)

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 _____

Helen Burgoyne
Marketing Manager
Halesowen College
Whittingham Road
Halesowen
West Midlands
B63 3NA

GDPR Steering Group Terms of Reference

1. Role/Purpose

The role of the GDPR Steering Group is to provide strategic direction and leadership to ensure that Halesowen College is as compliant as practically possible with the General Data Protection Regulations.

2. Term

The Terms of Reference are effective from 1 September 2021 and will be on going for the foreseeable future.

3. Membership

The Steering Group will comprise of:

Jacquie Carman (Data Controller)
Jon Priest (Information Services)
Rachael Charles (Personnel)
Matthew Davies (Software Development Team)
Ruth Broome(Registrar/Data Protection Officer)
Helen Burgoyne (Marketing)

4. Roles and Responsibilities

The Steering Group is responsible for promoting and ensuring that everyone is adhering to the GDPR.

The members will commit to attending as many meetings as possible and will suggest a substitute to the DPO if they personally are not available.

Members will be actively involved in meeting discussions.

5. Meetings

Where possible, all meetings will be chaired by the Data Controller or Data Protection Officer.

Meeting agendas minutes will be provided.

Meetings will be held once per term.

6. Amendment, Modification or Variation

This Terms of Reference may be amended, varied or modified in writing after consultation and agreement by the Data Protection Officer and Data Controller.