# Data Protection Policy

## Introduction

Halesowen College (the College) needs to collect and use personal data 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. The use of personal data by the College is regulated by data protection legislation: the UK General Data Protection Regulation (the UK GDPR) and Data Protection Act 2018 (DPA).

The College is the data controller in respect of the personal data it processes because it determines the purposes and means of processing.

This Policy should be read in conjunction with the included appendices.

## 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. Special category personal data is 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.

Special category personal data and data relating to criminal convictions and offences require higher levels of protection due to the sensitive nature of this data. The College will only process this information where it is legal to do so.

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

## Processing

The UK 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 creating, collecting, organising, amending, retrieving, using, disclosing, erasing or destroying personal data.

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

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

## 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. The UK sets out six data principles that must be complied with when processing personal data.

Specifically, the principles require that personal data is:

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;

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

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

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 is processed;

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.

To comply with its obligations under data protection legislation, the 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.

For practical advice on these principles, please see Appendix 1.

## Lawful Processing

In order to process personal data, the College must identify and document the legal basis for doing so. In order to be lawful, the College must comply with one of the following conditions for processing set out in the UK GDPR:

- 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; or
- 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.

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 and can be withdrawn at any time. Silence, pre-ticked boxes or inactivity will not constitute consent.

When processing special category 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 data set out under the UK GDPR. These include:

- Explicit consent of the data subject. Data protection legislation does not define 'explicit' but it is likely to mean consent that is specific, informed and given in writing.
- 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. Substantial public interest is exhaustively defined by the DPA and includes processing special category personal data for safeguarding purposes.
- 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 or where special category data has not been disclosed at that point, prior to or at the point of processing.

## Rights of data subjects

The UK GDPR provides data subjects with several rights in relation to their personal data, including:

- 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 in certain limited circumstances.
- 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 based on an automated process, including profiling, which has significant consequences for a data subject.

Please note that the right to erasure and the right to restrict processing are not absolute rights. The College will consider all requests against the valid reason and will comply with data protection legislation. This may mean retaining information for archiving purposes in the public interest.

## Subject Access Requests

One of the most important rights of data subjects is to know what personal data about them is being processed and to whom such personal data may be disclosed so that they are aware of and can verify the accuracy or lawfulness of processing. Individuals may request access to their personal data held by the College (a “subject access request”).

Requests should be made to the DPO; however, it is important to note that the UK GDPR does not set out formal requirements for a valid subject access request. Therefore, an individual can make such a request in writing, verbally, on social media, etc. A subject access request can be made to any part of the College and data subjects are not required to direct it to a specific person or contact point, therefore it is vital that College staff are able to identify subject access requests that may be made other than to the DPO.

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 to 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 its data protection obligations. Requests for information must be actioned as soon as possible and always within one calendar 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.

Individuals are entitled only to their own personal data and not to information relating to others. 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.

If a subject access request for personal data relating to an individual is submitted by a third-party, personal data should not be disclosed unless the data subject has given consent for the third-party to submit the request on their behalf. Written authority from the data subject concerned should therefore be requested before the request is processed.

Usually for students at the 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. Where the student is under 18 and there are safeguarding concerns, it may be appropriate to share information with the parent/guarding but any issues or concerns must be discussed with the Safeguarding and Inclusion Manager before disclosure is made.

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, the request can be refused or 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.

## Responsibilities

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

- **Data Protection Officer (DPO) 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, considering the nature, scope, context and purposes of the College's processing of personal data;
  - deal with requests from individuals to access the personal data Halesowen College holds about them (subject access requests);
  - check and approve any contracts with third parties who may process personal data on behalf of the College;
  - report to the Corporation (the College's governing body) on data protection issues.

- **The Chief Information Officer will support the DPO and is responsible for:**
  - ensuring all systems, services and equipment used for storing data meet acceptable security standards;
  - making certain that security hardware and software is functioning properly;
  - evaluating third party services to store or process data, for example cloud computing.

- **Staff are responsible for:**
  - Ensuring that personal data is shared only when it is justified. Special category 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;
  - attending all training provided by the College to help them understand their responsibilities when handling data;
  - forwarding all subject access requests to the DPO as soon as they are received;
  - reporting any suspected or actual personal data breaches to their line manager and DPO as soon as the breach is recognised;
  - keeping all data secure, by taking sensible precautions and following the guidelines.
  - setting strong passwords of at least six alpha numeric digits, mixed case and with a special character and never sharing their passwords;
  - storing data in line with the College's retention of documents policy, which can be accessed from http://data.halesowen.ac.uk/reports;
  - requesting help from their line manager or the DPO if they are unsure about any aspect of data protection;
  - not sharing personal data on platforms such as Teams.

## Transparency, fairness and accountability.

Data protection legislation 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 DPO;
- the purposes for which 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 UK and adequacy of safeguards;
- the intended retention period and any clauses affecting it;
- their subjects' rights in relation to their personal data;
- 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.

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 requirements outlined above.

## Data Protection Impact Assessments (DPIAs)

The College will conduct a DPIA when using new technologies where the processing is likely to result in a high risk to the rights and freedoms of individuals. Such processing 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; and
- the measures in place to address risk, including security and to demonstrate that compliance.

A DPIA can address more than one project.

## Data Security Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

It is important for the College to take all reasonable steps to prevent personal data breaches from occurring and to promptly address any personal data breaches that do occur. Serious breaches, if unaddressed, may have a significant detrimental effect on individuals – for example, they could 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 within 72 hours of becoming aware of a personal data breach where it poses a risk to the rights and freedoms of individuals. The UK 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. Whether a personal data breach results in a risk to the rights and freedoms individuals must be assessed on a case by case basis and the decision to report to the Information Commissioner will be made by the DPO.

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, unless the College had taken steps to render the personal data unintelligible (e.g. encryption) or has taken subsequent steps to ensure that the high risk to individuals is no longer likely to materialise. 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 DPO will decide whether the data subject should be informed.

If a member of staff suspects or becomes aware of a personal data breach, they must notify their line manager and/or the DPO immediately. Staff must take all steps requested by the DPO to contain the data breach and co-operate with any investigation or instruction given by the DPO or the Information Commissioner in relation to the breach.

## Code of Practice

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

- comply with data protection law regarding the collection and use of personal data and to specify the purposes for which personal data is processed;
- collect and process personal data only to the extent that it is needed to fulfil the purposes for which it was obtained or to comply with any legal requirements;
- ensure the accuracy and quality of personal data processed ensuring all necessary corrective action is taken expediently;
- apply strict checks to determine the length of time personal data, including imagery, is held and to comply with the retention periods so determined;

- ensure that the rights of individuals 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 UK unless there are UK adequacy regulations that cover the country where the receiver is located, or appropriate safeguards are in place (such as an international data transfer agreement as issued by the Information Commissioner) or a certification mechanism applies;
- observe and understand derogations in the UK GDPR.

## Useful Contacts

Assistance regarding data protection issues can be obtained within College from the following staff:

- Andrew Woodford, Vice Principal/Chief Finance Officer, ext
- Mark Garrett, Operations Manager & Data Protection Officer, ext 7620
- Rachael Charles Director of HR ext 7814
- Kate Woodford Personnel Manager ext 7644
- Jonathan Priest, Chief Information Officer, 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).

### Complaints

Any complaints concerning the College's processing of personal data should be addressed to the Data Protection Officer at **foi@halesowen.ac.uk** in the first instance who will investigate the complaint and make a response.

If you feel your complaint has not been properly addressed, complaints can be referred to the Information Commissioner.

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

The Information Commissioner's helpline is 0303 123 1113.

**APPENDICES**

Appendix 1 Practical Advice on Data Protection Principles
Appendix 2 Data Protection and CCTV
Appendix 3 Data Security Summary Guidelines
Appendix 4 Releasing Information to Prevent or Detect Crime
Appendix 5 Use of Photographs/Images

| Reviewed/Approved | By | Date |
|---|---|---|
| Updated by | Jacquie Carman/M. Davies/M. Garrett | 07.09.2023 |
| Approved at | CLT | 12.09.2023 |
| Website | Yes / No | Yes |
| Date of Next Review | | 01.09.2024 |

## Appendix 1

# 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 UK GDPR's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;
- notifying the Information Commissioner where required; 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

Because there is a right in relevant circumstances to have incomplete personal data completed, staff should ensure that they have sufficient personal data relating to individuals if important judgments are being made about them.

**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 Appendix 3 for more information)

**7 Personal data shall not be transferred to a country or territory outside the UK, 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 UK. The transfers will take place when someone outside the UK 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 UK, then this is a transfer. Such transfers need to comply with the requirements of the UK GDPR.

**Appendix 2**

# 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 data protection legislation.

## Purpose of CCTV

The College uses CCTV around our site as outlined below. We believe that such use is necessary in our legitimate interest, including:

- to ensure the health and safety of staff, students, visitors and other members of the public;
- to deter crime and protect buildings and assets from damage, disruption, vandalism and other crime;
- to support law enforcement bodies in the prevention, detection and prosecution of crime;
- to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings; and
- to assist in the defence of any civil litigation, including employment tribunal proceedings.

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

Operators of the equipment must only use 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.
- The College will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) except in highly exceptional circumstances where there are reasonable grounds to suspect criminal activity or extremely serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue. 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.
- CCTV 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 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 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 CCTV system is working properly.
- A maintenance and service log of the CCTV system shall 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 7 and 21 days unless required for a specific purpose.
- Once either the retention period has expired or the storage capacity of the CCTV system/device has been reached, 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 manually retained images, relating to an alleged or actual incident, should be kept in a secure location within either the CCTV Management System or designated CCTV Storage Repository. 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. Images retained for use as evidence or reference will be stored in a designated and controlled CCTV Storage Repository. Access to retained images within the storage repository, where appropriate, shall be primarily provided via restricted, self-expiring links which can only be used by the relevant authorised individuals for the duration covered by the associated request or investigation.
- 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 performed on any web-enabled College device using a secured connection to the CCTV Management System. The retrospective viewing of recorded images should only take place in designated areas (e.g. 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 Requests Spreadsheet 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 Requests Spreadsheet should be updated. 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 third-parties where we consider that this is reasonably necessary for any of the legitimate purposes described in the paragraph "Purpose of CCTV":

  - security organisations;
  - service partners and professional advisers;
  - persons making a data protection enquiry (subject to relevant restrictions);
  - police.

  for the purposes defined above. Again, a CCTV request should be made to the appropriate member of staff. A copy of every completed CCTV request will be held in the CCTV Requests Spreadsheet. Access to retained images when requested, shall be primarily provided via restricted, self-expiring links which can only be used by the relevant authorised individuals for the duration covered by the associated request. These will be stored on a CCTV SharePoint and can be deleted by the appropriate staff who reside over CCTV. In the case of Police requests to CCTV, the Evidence Share Requests that Police send have now replaced Data Release Forms and the portal where CCTV evidence is submitted covers UK GDPR as the previous forms did. All requests are kept in the CCTV Requests Spreadsheet along with the relevant share request email which covers UK GDPR.

  Removal of images from the premises of the 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

**Compliance**

For staff, failure to comply with this Code of Practice may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

# Appendix 3

## 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

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. The more important it is that personal data is accurate, the greater the effort should be in ensuring its accuracy.

- 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.

# Appendix 4

## Releasing Information to Prevent or Detect Crime

There is an exemption under data protection legislation 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. 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.

It is important that information is not given out without ensuring that the exemption applies or that the person has the power they are purporting to have. Therefore, all requests of this nature should be directed to the DPO.

# Appendix 5

## Use of Photographs/Video

The Data Protection Act 2018 regulates the use of all personal data including photographs and recordings from which people can be identified.

Wherever photographs or video may be taken for use in marketing material, clear indication should be given that photographs and or recordings will be taken and the purposes for which they will be used, so that individuals can object if they wish. Objections and ah-hoc consent will be recorded whenever provided. This will include signs in the relevant areas whenever possible indicating the areas the photography and or recording is taking place and providing clear information about what the footage will be used for.

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 captured images, photographs and video in marketing materials. Students have the option to provide or withdraw consent at any time during enrolment, progression, and census processes undertaken whilst at the College or by contacting the College's Data Protection Officer in writing. The status of a student's consent as to the use of their image is stored and maintained within the College's MIS (Management Information System) and is made available to relevant data processors for the purpose of determining consent when necessary.

Images may be used on the College website and other appropriate digital platforms which the College uses for marketing purposes. Images and or recordings used on these platforms will feature appropriate alteration (e.g., blurring of College ID cards) when necessary, to protect PII (Personally Identifiable Information) of any relevant subjects. Data protection law 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 the age of 16.