WORCESTER SIXTH FORM COLLEGE

DATA PROTECTION POLICY

Reviewed April 2016

MWK

WORCESTER SIXTH FORM COLLEGE

DATA PROTECTION POLICY

Purpose

This policy expresses Worcester Sixth Form College's statement of intent towards the responsible compliance with the Data Protection Act 1998 ('the Act').

The College needs to collect and process information including personal information about the people that it deals with in order to operate effectively and efficiently. This may include; Staff, Contractors[1], Students, Customers and Suppliers.

All personal data collected must be processed in accordance with the Act; this applies equally to data recorded electronically, paper files and other storage media such as CCTV.

To ensure the lawful processing of personal information, the College will comply with the data protection principles set out in the Act, which state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- Be adequate, relevant and not excessive for those purposes
- Be accurate and kept up to date
- Not be kept for longer than is necessary for that purpose
- Be processed in accordance with the data subject's rights
- Be kept safe from unauthorised access accidental loss or destruction
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The College and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the College has developed this Data Protection Policy.

Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees and contractors will abide by the rules and policies made by the College from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated data controller initially. If the matter is not resolved it should be raised as a formal grievance.

[1] For the purposes of the remainder of this document references to staff should be taken to also include contract staff.

Notification of Data Held and Processed

All staff, students and other users are entitled to:

- Know what information Worcester Sixth Form College holds and processes about them and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what the College is doing to comply with its obligations under the Act.

The College will ensure that management controls are in place to:

- maintain an accurate and up to date Notification of processing purposes;
- comply with the fair processing code regarding the collection and use of the data collected;
- maintain the quality and accuracy of data held and processed;
- review the retention periods for which data is reasonably retained;
- fully meet the rights of the data subject regarding data held and processed by the College;
- take appropriate technical and organisational measures to protect personal data from unauthorised or unlawful processing and accidental loss, destruction or damage;
- protect personal data from transfer outside of the EEA or where such transfer is necessary provide for adequate security of the information.

To ensure the effective application of the principles of the Act, the College will ensure that:

- there is a nominated data co-ordinator within the College with the specific responsibility for data protection;
- all persons processing personal data on behalf of the College receive adequate and periodic awareness training to ensure that they understand:
  - their contractual and legal responsibility towards the personal information processed by the College;
  - the procedure for responding to a request for data subject access or enquiries about the responsible handling of personal information;
  - the procedure for responding to a request for personal information held by the College, made by third parties / persons who are not the data subject;
- adequate management supervision is in place for the processing of personal information;
- the methods for handling and managing personal information collected and processed by the College are periodically reviewed.

The College will also ensure that wherever possible it adheres to the guidance provided by the Information Commissioner in the Employment Practices Data Protection Codes of Practice to assist in the fulfilment of our Data Protection Act obligations.

Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to the College in connection with their employment is accurate and up to date
- Informing the College of any changes to information, which they have provided, i.e. changes of address
- Checking the information that the College will send out from time to time, giving details of information kept and processed about staff
- Informing the College of any errors or changes to their personal data.

In order to ensure the accuracy of staff data the College will provide all staff at least annually with a standard form of notification for completion and return.

If and when, as part of their responsibilities, staff collect information about other people (i.e. about potential staff, students etc, opinions about ability, references to other employers, or details of personal circumstances), they must comply with the guidelines for staff which are at Appendix 1.

Student Obligations

Students must ensure that all personal data provided to the College is accurate and up to date. They can verify that this is correct by using the College Gateway and should ensure that changes of address are notified to the Tutorial Hub.

Students who use the College Computer System should not process personal data without special approval of the IT Support Manager.

Data Security

All staff are responsible for ensuring that:
- Any personal data which they hold is kept securely
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party
- Any suspected breaches of security are notified to the IT Support Manager.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should be:
- kept in a locked filing cabinet or drawer
- saved on the College network in an appropriate place i.e. NOT student area
- kept only on an USB Stick or External Hard Drive which is encrypted and/or password protected

Further guidance on Information Security good practice is provided at Appendix 2.

Rights to Access Information

Staff, students and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the College's "Access to Information" form and forward it to the nominated data co-ordinator. See Appendix 3.

The College will make a charge to staff and students of £10 on each occasion that access is requested, although there is discretion to waive this as may be agreed by the Principal.

The College aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 40 days of receiving the request unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

Individuals also have certain rights under the Act to require the College to cease processing or using their personal information in certain circumstances. Further information will be provided if required.

Publication of Worcester Sixth Form College Information

Information that is already in the public domain is exempt from the Act. It is the College's policy to make as much information public as possible, and in particular the following information will be available for inspection:

- Name and contact address of the College's Governors

- List of key staff
- Annual Report and accounts.

The College's internal phone list and staff emergency contact information will not be public documents.

Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the designated data co-ordinator.

Subject Consent

In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, **express consent** must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

Some jobs within the College will bring the applicants into contact with children, including young people between the ages of 16 and 18. The College has a duty under the Children Act and other enactments to ensure that staff are suitable for the job offered. The College also has a duty of care to all staff and customers and must therefore make sure that employees and those who use the College's facilities do not pose a threat or danger to other users.

The College will also ask for information about particular health needs, such as allergies to particular forms or medication, or any conditions such as asthma or diabetes. The College will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

Therefore, all prospective staff and contractors will be asked to sign a 'Consent To Process' form, regarding particular types of information when an offer of employment is made. A refusal to sign such a form can result in the offer being withdrawn.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure the College is a safe place for everyone, or to operate other College policies, such as sickness payments or the equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the College to do this. Offers of employment may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the data co-ordinator and from line managers.

Examination Marks

Students will be entitled to information about their marks for both coursework and examinations. However this may take longer to provide than other information.

The Data Controller and the Designated Data Co-ordinators

The College as a body corporate is the data controller under the Act, and the Governing Body is therefore ultimately responsible for implementation. However, the designated data co-ordinator will deal with day to day matters.

The College has a designated data co-ordinator. This is Matt Broderick, IT Support Manager.

Data Processors

A data processor is defined in the Act as "any person other than an employee of the data controller who processes data on behalf of the data controller."

The College must ensure that any data processor or any third party of the data processor will not misuse the data or process it any way incompatible with the College's specified and lawful purpose for that data. Therefore adequate controls must be in place, and relevant wording included in contracts with all data processors and third parties (more detailed information can be found at Appendix 5, or contact the data co-ordinator for advice).

Retention of Data

The College will keep some forms of information for longer than others. Appendix 4 gives the retention period for different types of data.

Advice received via the SFCA about employees is that data required for preparation of employment references should be kept indefinitely for reasons of child protection.

In general information about students will be kept for a maximum of 12 years after they leave the college. This will include:

- name and address
- academic achievements
- copies of any references written

The destruction of personal data which may consist of both manual and computerised records will be dealt with in a secure manner either through in-house shredding or through the services of an appropriate contractor.

Use of CCTV

The College use of CCTV must be used in accordance with the Data Protection Act 1998 (DPA) and accessed and used in accordance with this policy.

CCTV is present on the College site externally, internally in corridors, workspaces, classrooms and student common areas, and care should be taken as the reasons to access CCTV may differ between locations.

Automatic number plate recognition (ANPR) is also used on the College site, and consideration needs to be made in relation to the storing and accessing of the collected data.

Current placement of cameras including justification and impact

External cameras covering:

- car parks and bike sheds

    - for the purpose of security, enforcing safe driving, Safeguarding and Prevent
    - privacy impact low – neighbouring properties shielded by foliage, no live monitoring
- vehicle access barrier
    - for granting access for non-card issued drivers
    - privacy impact low – limited field of vision, monitored when access request by driver using intercom
- access drive
    - for the purpose of ANPR to ensure the College can identify cars involved in incidents, for identifying unusual activity of non-registered vehicles on the grounds of Safeguarding and Prevent
    - privacy impact medium – separate system to minimise access to logging, camera sited with focus on private road
- rear of site in student common area
    - for purpose of building security, deterrent to unauthorised persons and to identify students involved in incidents of significant misbehaviour
    - privacy impact medium – cameras for person identification are focused on access gates, cameras coving recreation areas, no live monitoring

Internal cameras covering

- entrances to building
    - deterrent to unauthorised persons, identification of persons entering the building without permission
    - privacy impact low – cameras are focused on doors, no recreation or workspaces covered, no live monitoring
- outside student toilets
    - deterrent to and identification of persons conducting vandalism and/or bullying, Safeguarding
    - privacy impact low – cameras are focused on person exiting toilets and afford no view into toilet areas and cover no recreation or workspaces, no live monitoring
- classroom entrances
    - deterrent to and identification of persons conducting theft and vandalism
    - privacy impact low – cameras are focused on person exiting and cover no workspaces, no live monitoring
- workspaces
    - identification of unauthorised access of staff and students
    - privacy impact medium – cameras not focused on workstations, high value of goods and security of systems storing data
- student common areas
    - deterrent to and identification of persons conducting vandalism, bullying or violence
    - privacy impact medium – cameras are focused on recreational areas, only to be used for serious incidents, no live monitoring
- restricted access common area
    - Safeguarding under 16 year olds studying at the College outside of lessons
    - privacy impact medium – cameras focused on door not recreation areas, live monitored

Justification for siting camera

Just because a camera location is possible and affordable are not suitable justification for processing personal data. Regarding the nature of the issue being tackled consider:

- justification
- effectiveness
- alternative solutions
- effect of individuals

Example from ICO: Cars in a car park are frequently damaged and broken in to at night. Consider whether improved lighting would reduce the problem more effectively than CCTV.

Camera should be sited to ensure wherever possible that areas that are not of interest and are not intended to be subject to surveillance are not captured. Camera recording is restricted by time or motion in specific areas in line with the justification for placement.

Governance
Access to video, images and ANPR data will be made in accordance with the **Procedure for accessing CCTV footage** with a requests being made by an authorised person (members of SMT, HoYs or the IT Support Manager), other members of staff to be directed to seek permission from an authorised person, and persons representing law enforcement to the Principal.

Wherever possible, access will be made by two members of staff, using a location that affords adequate privacy, with consideration of impact on the person accessing in relation to incident reported. Incidents of a serious nature or potentially involving staff should be accessed by the IT Manager and a second person of relevant seniority.

A record of access will be made and stored securely with a copy of any relevant material on USB or DVD.

Subject access requests
Individuals whose information is recorded have a right to be provided with that information or, if they consent to it, view that information. Information must be provided promptly and within no longer than 40 calendar days of receiving a request.

Those who request access must provide you with details that allow you to identify them as the subject of the information and also to locate the information on your system.

The College is required to provide the data subject with a copy of all the information caught by the request that constitutes their personal data, unless an exemption applies. This must be done by supplying them with a copy of the information in a permanent form, unless the data subject agrees to receive their information in another way, such as by viewing the footage.

If the footage also has third parties, it may be appropriate to release information to a third party, where their needs outweigh those of the individuals whose information is recorded. Otherwise you need to consider whether the identifying features of any of the other individuals in the image need or can be obscured, it mean that still images can be released but not video.

Retention
The DPA does not prescribe the retention periods, so retention will be determined by available storage, unless a specific reason for specific set of camera is subsequently decided. ANPR data is recorded for identifying vehicles involved in incidents identified from CCTV, which would stipulate holding it for approximately 2 weeks, however the College will retain the data for identifying uncharacteristic behaviour on the grounds of Safeguarding and *Prevent*, unregistered vehicles parking on site.

Conclusion

Worcester Sixth Form College has a statutory responsibility to ensure compliance with the eight principles of the 1998 Act. There is therefore a responsibility for compliance placed on staff and personal liability may arise where irresponsible or negligent non-compliance occurs. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated data co-ordinator.

Appendices

1. **Staff Guideline for Data Protection**
2. **Information Security Good Practice Guide**
3. **Data Processor Relationships Guide**
4. **Retention of Data Guidelines**
5. **Access to Information Form**
6. **Student Data Protection Statement**
7. **Data coming under the category of Sensitive Personal Information in the Data Protection Act 1998**
8. **Automatic Number Plate Registration CCTV**

Appendix 1

Staff Guidelines for Data Protection

1. All staff will process data about students on a regular basis, when updating transaction systems, writing reports or references, or as part of a pastoral or supervisory role. The College will ensure through registration procedures, that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the Act.

2. Information about staff or student's physical or mental health; sexual life; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the data subjects consent. Staff and student application forms contain statements giving consent to this.

3. All staff have a duty to make sure that they comply with the data protection principles, which are set out in the Data Protection Policy. In particular, staff must ensure that records are :
   - accurate;
   - up-to-date;
   - fair;
   - kept and disposed of safely, and in accordance with the policy.

4. Staff will be responsible for ensuring that all data is kept securely.

5. Staff must not disclose personal data to any third party without authorisation or agreement from the data co-ordinator, or in line with the College's disclosure policy. The College has ultimate responsibility for the information it processes and should not disclose data in any circumstances without reasonable justification.

6. Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated data controller, or in line with College policy.

9. Before processing any personal data, all staff should consider the checklist.

Appendix 2

Information Security – Good Practice Guidance

What is information security?
Information can be defined as an important business asset of the College, which like all other assets will have a value. The value of personal information coupled with a dependency on the systems which process the information means that it must be afforded adequate protection from the wide ranging threats which may affect it and result in unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Information security can be defined as covering three core principles:

- **Confidentiality:** Ensuring that information is accessible only to those authorised to have access;
- **Integrity:** Safeguarding the accuracy and completeness of information and processing methods;
- **Availability:** Ensuring that authorised users have access to information and associated assets when required.

Password Security
Passwords provide a means of validating a user's identity and thus to establish access rights to information processing facilities or services. Users should follow good security practices in the selection and use of passwords.

For example:
- Passwords should be easy for the user to remember but difficult to guess by anyone else
- Set quality passwords of at least 6 characters using a mixture of upper and lower case characters, and include the numeric and non standard character set
- Keep passwords confidential
- Do not share your password with any other user
- Change your password and inform your data co-ordinator immediately if you believe your password has been compromised.

Clear Desk, Secured Computer or Locked Door Policy
In order to reduce the exposure to risk arising from unauthorised access, loss of, and damage to personal information during and outside normal working hours staff should:

During the working day:
- When leaving a workspace lock the office or tidy away to a locked draw or filing cabinet any confidential paper or digital storage
- Ensure the computer is off or in a secured state or the office door is locked
- Clear the computer screen of personal information if visible to unauthorised persons

Outside of the working day:
- Where feasible tidy away to a locked draw or filing cabinet any confidential paper or digital storage
- Where practical the computer is off or at least in a secured state

Staff should also ensure:

- Any sensitive or confidential information printed must be removed from the printer immediately and securely destroyed if not required.
- Computer screens are not routinely visible to unauthorised persons

Responding to Security Incidents
A security incident may be defined as any event that has resulted, or could result, in:

- The disclosure of personal, sensitive or confidential information to any unauthorised individual
- The integrity of the College's systems or data being put at risk
- An adverse impact, for example
  - Financial loss
  - Errors resulting from incomplete or inaccurate data
  - Disruption of activities and Denial of service incidents
  - Information system failure or Loss of service
  - Embarrassment to the College
  - Threat to personal safety
  - Any Legal obligation or penalty.

Any suspected security incident must be reported to the designated data co-ordinator, the reporting of any incidents will be treated in confidence if necessary.

Backups
It is important that there are procedures in place to maintain the availability of data and Information and the integrity of information being processed in the event of failure.

Core systems will be backed up automatically as part of the College's IT processes.

Viruses
Viruses and other malicious code can have a devastating effect on the information and service continuity of the College. It is important that users bear in mind the following points of good practice:
- No software should be installed without prior consent from the IT Support Manager, IT Senior Information Officer or IT Support Technical coordinator
- Do not download software or files of an unknown origin from the Internet
- Do not open attachments on emails from unknowns sources
- Inform IT Support immediately if you believe your PC has a virus, as it may also be on your USB stick or external hard drive.

Electronic Transmissions
It is important that staff recognise the risks associated with electronic transmission of data and take the appropriate precautions when sending personal, sensitive or confidential information by electronic methods. It is the responsibility of the College to ensure the security of personal information processed is afforded adequate protection.

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 of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Staff should consider the following good practice points for electronic transmission.
- Never disclose personal information over the phone, even if the caller appears genuine or claims to be from the Police or a Government Executive Agency.
- Check before you send a fax containing personal or sensitive information, if the intended recipient fails to collect the fax or the number is incorrect, the College or the individual may be held responsible for unlawful disclosure.
- Be careful about what you send via email and who you send it to. Email and the Internet are world-wide resources, and transmitting information via this means has no guarantee that the routing of your message will not take it outside of the EEA. It is important that staff ensure that email and the Internet (only submit data to sights with a valid HTTPS certificate – consult IT Support for guidance) is not used inappropriately and confidential or sensitive data inadvertently put at risk of interception outside of the EEA.

Finally: If in any doubt contact the designated Data Co-ordinator, Matthew Broderick.

Appendix 3

Standard Request for Access to Data

Access to Information Form
Thank you for your request for access to the personal data we hold about you. To enable us to process your request, please complete the enclosed form and return it to us along with one of the identification documents listed below, and the appropriate fee. Completion of the form, while not compulsory, will help us to provide you with the information you require quickly and fully.

Identification

A passport or driving licence (that has a photo) or any two of documents listed below may be used for this purpose:

- a bank, building society or credit card statement
- a utility bill.

The document must be an original, not a photocopy, dated within the last 3 months. It must show your full name or first initial and surname and your current address. All documentation will be returned to you once your identity has been verified.

If you are unable to provide any of the above items, please attach a letter confirming your identity. This must be an original, typed on headed paper, dated within the last three months and authenticated with an official stamp if applicable. It should be from your employer, solicitor or other professional body or person.

There is normally a charge of £10 for this service. Please send a cheque made payable to Worcester Sixth Form College.

……..

Access to Information Form

I, _____ wish to have access to either (delete as appropriate)

A. All the data that Worcester Sixth Form College currently has about me, either as part of an automated system or part of a relevant filing system;

Or

B. Data that Worcester Sixth Form College has about me in the following categories :

Personal details including name, address, date of birth etc	☐
Employment references	☐
Disciplinary records	☐
Health and medical matters	☐
Political, religious or trade union information	☐
Any statements of opinion about my abilities or performance	☐
Any academic or development information	☐
Other information	☐

[Please tick as appropriate]

Signed _____ Dated _____

Appendix 4

Retention of personnel records for Data Protection Act 1998 compliance

Type of Record	Retention period* before secure disposal
Application forms and interview notes (make sure interview notes have been recorded on EO monitoring before destroying)	1 year
Speculative enquiries	1 year
Pool of staff	3 years
Ex staff personnel files – manual and electronic (except senior management which will be kept permanently for historical reasons)	6 years (unless child protection issues - not to be destroyed)
PDR central records	5 years
Lieu or additional hours sheets	2 years
Holiday request sheets	2 years
Absence and return confirmation sheets, including copy medical certificates	4 years
Unpaid leave request sheets	4 years
Support staff standards payments applications	3 years
Staff data checks	3 years (unless declaration affecting contractual terms – keep in personnel file)
Equal opportunities monitoring forms	1 year (entered on spreadsheet before disposal)

*All retention periods refer to a minimum number of years, prior to an annual secure disposal process.

References provided by Worcester Sixth Form College (WSFC): manual copies are disposed of with the personnel file, electronic copies since approx 2000 are kept on file for the potential benefit of the member of staff, unless specifically requested by them not to do so.

Prior to disposing of personnel files, the following information will be kept on file to enable future confirmation of employment at WSFC in the event of reference or Freedom of Information requests:

A spreadsheet of leavers containing:

- surname and first name
- date of birth
- last job title
- post type - support or teaching staff
- dates of work (start and end dates, though whether or not this was continuous employment will not be recorded).

The record commences with leavers from April 1993 when WSFC became incorporated.

All requests for data held prior to April 1993 should be redirected to Worcestershire County Council, which was the employer at that time.

Retention of student records for Data Protection Act 1998 compliance

Student records (including academic achievements and conduct) will be retained for at least 6 years from the student's leaving date.

Unless the student requests otherwise, student information will be retained for at least 10 years for the purpose of personal and academic references.

Appendix 5

Data Processor Relationships

A data processor is defined in the Act as "any person other than an employee of the data controller who processes data on behalf of the data controller."

The definition of processing under the Act is far wider than before and now includes almost any action in connection with personal data. A data processor could therefore be performing almost any function involving personal data on behalf of the data controller from obtaining and holding to disclosure and destruction. It is therefore likely that all organisations will have data processors in some form and consideration should be given to the following:

- Outsourced data processing contracts i.e. payroll administration
- Support and Service contracts i.e. System Support
- Office cleaning contractors
- CCTV contracts
- Waste disposal services
- Mailing houses
- IT contractors
- Couriers
- Agency staff

When the College uses services such as those listed above (they are by no means exhaustive), it is essential that as the data controller they can place reliance that the data processor or any third party of the data processor will not misuse the data or process it any way incompatible with the data controllers specified and lawful purpose for that data.

Data processors are distinguished from data controllers because they do not exercise control over the way in which personal data they handle is processed. They do not determine the purposes for which data is processed although they may to a certain extent determine the manner in which data is processed.

This distinction between the College as ultimate data controller and the data processor must be clearly understood because only a data controller has any direct obligation to comply with the requirements of the Act. In effect it means that the data controller will be liable for any breach of the Act which occurs while its data is in the hands of a data processor.

Before entering into a contract with a data processor the College must ensure that the data processor can offer "sufficient safeguards" with respect to the data being processed.
The College will require assurances that the data processor has adequate technological and organisational procedures in place to protect data being processed, from unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, the data.

With regard to contracts for the processing of personal data on behalf of the College, (for example for payroll services). The College must ensure the following:

- that the data processor provides sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out
- that they take reasonable steps to ensure compliance with those measures
- that the processing is carried out under a contract in writing and under which the data processor is to act only on instructions from the College.

It should be noted that this will apply to existing contracts where it is recommended that a suitable letter is exchanged seeking to impose the obligation for data processors to guarantee the technical and organisational security of data. Any new or renewed contracts should have an appropriately worded clause added to the contractual agreement.

Appendix 6

Student Data Protection Statement

This statement is updated annually and new applicants see this every time they log on to their online application.

Appendix 7

Data coming under the category of Sensitive Personal Information in the Data Protection Act 1998

- the racial or ethnic origin of the data subject (an individual who is the subject of personal data)
- his political opinions
- his religious beliefs or other beliefs of a similar nature
- whether he is a member of a trade union (within the meaning of the [1992 c.52] Trade Union and Labour Relations (Consolidation) Act 1992)
- his physical or mental health or condition
- his sexual life
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

NB Please note that the College does not process all of the above data

Examples of reasons for which this information may be processed:

- Payment of salary, pension, sickness benefit or other payments due under the employment contract
- Monitoring absence or sickness under an absence control or capability policy.
- Training and development purposes
- Management planning, recruitment and selection, redundancy and succession planning
- Negotiations with the trade union or staff representatives
- Compliance with legislation
- Carrying out checks through criminal records or other appropriate mechanisms

Text appearing on sign located on the entrance drive to the College regarding CCTV and ANPR

ANPR CCTV
CCTV and Automatic Number Plate Recognition is in operation for the purpose of identification of vehicles involved in incidents occurring on College property and to promote a safe environment for students, staff and visitors.
The scheme is operated by Worcester Sixth Form College
For more information please go to Visitor Reception or contact the College on 01905 362600