WORCESTER SIXTH FORM COLLEGE

GENERAL DATA PROTECTION REGULATIONS (GDPR) POLICY

April 2018

WORCESTER SIXTH FORM COLLEGE

DATA PROTECTION POLICY & PROCEDURES

Introduction
Worcester Sixth Form College ('the College') and all of its staff, governors and volunteers, process and protect personal data in accordance with the General Data Protection Regulation (GDPR).

Purpose
This policy sets out the College procedures for processing and protecting personal data.

The College when processing any personal data will:

- only do so where a specified, explicit and legitimate purpose exists;
- minimise how long we continue to process personal data whilst meeting our obligations as an education establishment and employer;
- endeavour to ensure inaccurate data is rectified and that personal data will be kept up to date;
- have procedures and practices in place that put first and foremost the security and the prevention of loss of personal data.

The lawful basis on which the College will process personal data is:

- a necessity to meet legal obligations as an education provider *Article 6(1)(c);*
- where it is necessary to provide students their education *Article 6(1)(e);*
- contractual when entering employment or during employment *Article 6(1)(b);*
- where explicit consent has been given by the data subject *Article 6(1)(b).*

The College, for the purposes of the GDPR and the lawful processing of data under *Article 6(1)(e)*, is considered to be a 'Public Authority' as defined in the Freedom of Information Act 2000.

The College when processing special categories of personal data will:

- only share the data with staff members where a specified and explicit purpose exists;
- minimise possible storage locations to reduce risk of data loss;
- only allow the data off of the premises when it is in the data subjects interest to do so (using encryption when appropriate);
- endeavour to ensure that staff members know who they can share the data with;
- have procedures and enhanced practices in place that prevents data loss or inappropriate sharing.

The lawful basis on which the College will process special categories personal data is:

- necessity for reason of substantial public interest *Article 9(2)(g).*

The following is indicative of the data the College processes

The categories of personal data the College will process about **students** include:

- personal information e.g. name, date of birth, contact details;
- personal information under special categories e.g. ethnic origin is required to monitor the distribution of ethnic groups amongst learners in the context of adequacy and sufficiency;
- academic activities and progress e.g. courses being studies and the marks obtained;
- attendance e.g. individual attendance at lessons, overall course attendance;
- exams e.g. entries on exams, timetables;

- exams under special categories e.g. medical information for special consideration requests;
- pastoral care e.g. memos from you tutor in supporting your study;
- pastoral care under special categories e.g. notification of absence could contain medical information;
- counselling services e.g. memos taken when seeing a counsellor;
- counselling services under special categories e.g. memo taken when seeing a counsellor about sexual orientation.

The categories of personal data the College will process about **someone applying to be a student at College** include:

- personal information e.g. name, date of birth, contact details;
- personal information under special categories e.g. medical information to allow the College to support you through the process;
- references supplied e.g. academic reference from previous school;
- evidence of eligibility for funding e.g. copy of passport.

The categories of personal data the College will processes about **employees** include:

- personal information e.g. name, date of birth, contact details;
- personal information under special categories e.g. medical information to allow the College to support employees in their work; performance management information to allow to College to maintain high levels of attainment for the benefit of its students;
- reference supplied e.g. employment reference from previous employer;
- evidence of right to work e.g. passport;
- evidence of staff development for the benefit of its employees.

The categories of personal data the College will processes about **governors**:

- personal information e.g. name, date of birth, contact details
- personal information under special categories e.g. register of interests to ensure there are no conflicts of interests;
- evidence of eligibility to act as a governor;
- evidence of training undertaken and requirements;
- evidence of appraisal to ensure that governors are undertaking their roles effectively.

The categories of personal data the College will processes about **volunteers**:

- personal information e.g. name, date of birth, contact details
- reference supplied e.g. employment reference from previous employer;
- evidence of right to work e.g. passport

Retention of Data

The College will keep some forms of personal data longer than others. This will depend upon the lawful basis on which the College has relied to process the data and the nature of the data itself.

The following example is given to illustrate this:

Student's personal information	7 years	Requirement of government funding agency
Student's individual attendance marks	Duration of study at College	Necessary to provide students their education
Personal and academic information relevant to write student references	7 years	Necessary to support students after provision of education

The Data Protection Officer (DPO) and College management reviews the personal data held by the College in its Information Asset Register on an annual basis. As part of this process the justification for processing and retaining data as well as the period of retention for the data is also reviewed.

The Information Asset Register is reviewed by the Resources Committee and approved by the Governing Body annually.

The specific period and justification for retention for any particular personal data is available on request from the DPO.

Definitions
For the purposes of this Regulation:

'Data processor' means the employees that process data on behalf of the organisation e.g. Admissions Assistant, Exams Manager, Personnel Officer.

'Data subject' means an identified or identifiable person

'Personal data' means any information relating to an identified or identifiable person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

'Processing of personal data' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'Third party' means a natural or legal person, public authority, agency or body other than the data subject, processor and persons who, under the direct authority of the College or processor, are authorised to process personal data;

'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

'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 transmitted, stored or otherwise processed;

The College will ensure compliance with its GDPR responsibilities by the following:

- adequate compliance processes and procedures are implemented and monitored;
- appropriate and regular staff training;
- implementation of technical and College data security measures;
- an appropriate legal basis for its data processing activities through a recorded audit process.

Responsibility of the College
The College's designated Data Protection Officer is Matt Broderick. The College's Governing Body is ultimately responsible for implementation and the Principal responsible for compliance. If you have concerns about personal data processed by the College or about a data loss, please contact the DPO via email (dpo@wsfc.ac.uk).

Subject Access Requests
Staff, students and other users of the College have the right to access any personal and sensitive data that is being kept about them. Any person who wishes to exercise this right should make a request in writing to the Data Protection Officer.

The College aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within one month of receiving the request.

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

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.

Arrangements with third party providers
Where the College does share information with third party providers this will only be to comply with legal requirements (e.g. funding bodies) or where it is in the interests of the person concerned (e.g. examination boards, safeguarding bodies) or where it is necessary for the provision of services (e.g. ParentPay). In all instances an appropriate data sharing agreement is in place.

High Level Data Security Measures
Examples of the data security measures that the College has in place include:

- Machine encryption;
- Use of encrypted USB sticks for transportation of personal data;
- Central deletion of emails;
- Specified retention measures.

College policies
In following policies should be consulted in conjunction with this policy due to the potential for data protection implications:

- Acceptable Use Policy
- Staff Code of Conduct
- Safeguarding Policy

Consequences of non-compliance
Any breach of GDPR regulations or non-compliance will be taken seriously by the College.

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 Data Protection Officer.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. This may also apply to data loss.

Use of CCTV
The College use of CCTV must be used in accordance with GDPR and accessed and used in accordance with the 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.
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.

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.

CCTV 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.

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

The College is required to provide the data subject with a copy of all the information covered 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.

Monitoring
The policy will be monitored annually by the Senior Management Team and the Data Protection Officer and will be reviewed annually by the Audit Committee and approved by the Governing Body.

Appendix 1

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

Appendix 2

GDPR: Procedures for staff

1, Introduction

I. All staff must ensure that any personal data they hold is kept securely. Where personal data is sensitive, staff are responsible for understanding the additional security protocols relating to the specific data and where it is stored.

II. It is the responsibility of all staff to ensure that any personal and sensitive information they process or store is identified in the College's Information Asset Register maintained by the Data Protection Officer.

III. Please clarify any of the above with the DPO if you are in any doubt.

IV. The procedures for the safe storage, access and processing of personal and/or sensitive data will be audited by the College.

V. Staff must not disclose any personal and/or sensitive data to any unauthorised third party.

VI. All staff must not disclose another person's personal and/or sensitive data to other members of staff, unless they know that person should also have access, except with the authorisation or agreement of the DPO.

VII. Any suspected breaches of data security must be immediately notified to the DPO.

VIII. Staff must ensure that records are accurate, up to date, fair and stored and disposed of safely and in accordance with the Information Asset Register.

IX. Staff must ensure that where appropriate offices are locked and any personal and sensitive information, paper or digital storage, is secured if the office is unoccupied.

2, Electronic records

Electronic files must be stored in the appropriate network area or on an encrypted memory stick or an encrypted hard drive.

A, Data about students held by Teaching* staff

(This will also apply to staff with similar functions such as Pastoral staff or Academic and Learning Support)

I. Teaching staff must store personal and/or sensitive data about students in the academic year folder on their G drive.

II. Where teaching staff need to share personal and/or sensitive data about students with other staff it must be stored in the academic year folder in the staff restricted area of their department files.

III. Where a document contains personal and/or sensitive data about an individual student it must contain the student's S number in the file name. Where the personal and/or sensitive data relates to more than one student, e.g. a teacher's record of marks and progress for a group of students, it must be cross referenced by the students' S numbers. These measures will enable to College to respond effectively to subject access requests without imposing a significant administrative burden on individual staff.

IV. Academic year folders will be created centrally by the College. They will also be retained and deleted centrally in accordance with the College's Information Asset register so as to ensure compliance and avoid a significant administrative burden on individual staff.

V. If a teacher processes or stores any personal and/or sensitive data about staff, e.g. while they are composing a letter to parents, they must save it in their confidential staff files. This must then be deleted once the data has been processed and stored in the agreed location.

B, Data held by Administration staff

I. Administration staff must save files containing personal and/or sensitive data about students or staff in an academic year folder in their relevant area of the admin drive on the College network.

II. Academic year folders will be created individually by Administration staff.

C, Data about staff held by line managers

If a line manager processes or stores any personal and/or sensitive data about staff, e.g. while they are working on a PDR, they must save it in their confidential staff files. This must then be deleted once the data has been processed and stored in the agreed location, for example staff PDRs will be forwarded to the individual member of staff and personnel.

D, General Principle's relating to the safe storage and use of data stored and secured electronically

I. Staff must use robust passwords on all devices used to store, process or access personal and/or sensitive data. If a member of staff believes that their password has been compromised, they must change it and inform the Data Protection Officer immediately.

II. Where staff have a need to save passwords, they are encouraged to use a Google account, and use Google's 2-Step Verification,

III. Where possible staff should use the cloud@WSFC rather than USB devices when transporting personal and/or sensitive data. Where a USB device is used this must be encrypted.

IV. Staff must ensure that computers are switched off or in a secured state if they are away from their machine.

V. Single user machines are protected by encryption that requires the relevant member of staff to use a USB encryption key when switching on their machine. The USB encryption key must not be left with the machine, copied or used for any other purpose. The USB encryption key must be kept attached to the member of staff's identity lanyard. This must be left in a secure place when staff leave the College premises, e.g. in the staffroom pigeon holes.

VI. Staff must not allow any other person to use their single user machine or a machine they are logged on to, or share logons to a device.

VII. Staff must not install software without prior consent from the IT Support Manager or download software or files of an unknown origin from the Internet

VIII. Staff must not open attachments to emails from unknown sources

IX. Staff must not connect a device to the College Wi-Fi that does not have up to date antivirus software installed or the latest security patches, or be a Jailbroken device.

X. Staff must not attach any device to the College network e.g. by using a network cable other than via the College Wifi network

XI. Staff must not join or attempt to join a device to the College domain

XII. Staff must not be in possession of software that could be used to violate the privacy of other users (such software includes, but is not limited to, port scanners, password crackers, remote machine monitors and network traffic sniffers)

XIII. Staff must not use a public WiFi connection to access College resources unless it is via a trusted VPN provider e.g. Avast VPN.

XIV. Staff must ensure that computer screens are not routinely visible to unauthorised person.

XV. If any member of staff finds a computer that has been left unsecured and unattended they must take immediate action to ensure it is secured, e.g. switch off or restart.

XVI. Staff must ensure that any sensitive or confidential information printed is removed from the printer immediately and securely destroyed if not required.

XVII. Staff must report any suspected security incident to the Data Protection Officer (the reporting of any incidents will be treated in confidence if necessary)

E, Email

I. Particular care must be taken with the use of email, both in ensuring the recipient of any personal and/or sensitive data is authorised to receive it and that they have adopted procedures that are compliant with GDPR. The steps to secure electronic data outlined above, are designed to allow staff to use email whilst minimising the risk of data loss or breach.

II. Carefully consider what you send via email and whom you send it to. Wherever possible do not send personal and/or sensitive information via email, avoid copying in people without clear and good reason and consider verifying the email address before sending it.

III. Staff must not use personal email accounts for work matters without the specific agreement of the DPO.

IV. Staff must not use work email accounts for personal use.

V. Teaching staff must follow the procedures for the safe processing, storage, and access of electronic files containing personal and/or sensitive data as outlined in the sections above. As a consequence of following these procedures teaching staff are able to attach files to emails with no additional restrictions.

VI. Administration staff with significant access to personal and/or sensitive data will be able to send emails with attachments once these have been verified by the staff identified for this purpose.

VII. Where an email contains a student's personal and/or sensitive data then the student's S number must be used in the email subject or its general content to avoid a significant administrative burden on individual staff when responding to subject action requests.

3, Paper records

I. Wherever possible staff must store, process and access personal and/or sensitive data electronically.

II. When staff make notes on paper containing personal and/or sensitive data for future discussion and/or processing they must use the confidential notes pad supplied by the College and immediately and securely destroy these notes once the matter has been actioned.

III. Where staff need to keep paper records or notes containing personal and/or sensitive data beyond the period required for discussion and/or processing, e.g. a teacher's records of students' marks, then they must do so securely. Such notes or records will constitute an Information Asset and must be kept in a labelled folder or diary. These records must then be submitted for archiving or destruction by the College in accordance with the Information Asset Register.

IV. Staff must ensure that folders and individual notes containing personal and/or sensitive data are stored securely and in line with the Information Asset Register, e.g. some data will require to be locked in filing cabinets and for the office to be locked when unoccupied.

V. Staff must only take a student's personal data off site if this is necessary in order to carry out their role effectively in the interests of students, for example teachers may need to have access to a mark-book when completing marking away from the College. In these circumstances they must take appropriate steps to maintain the security of the data.

VI. Students' sensitive data must only be taken off-site off site in agreed circumstances, for example attending a safeguarding meeting, when they must follow the agreed procedure for the safe transport and security of the data. In any other circumstance sensitive data must not be removed from College without the express permission of the DPO and the

member of staff must follow the DPO's instruction regarding the safe transport and security of the data.

These procedures should be considered in conjunction with the following policies:

- GDPR
- Staff Code of Conduct
- Acceptable Use Policy for Staff
- Freedom of Information
- Safeguarding

EYS 5/18

Appendix 3

Governors' Responsibilities

i. The Governing Body is responsible for monitoring and approving the College's GDPR policy.
ii. The Audit Committee is responsible for monitoring the College's procedures and compliance with GDPR requirements.
iii. A designated governor is responsible for ensuring that staff in general and, in particular, the Data Protection Officer, have a mechanism for reporting concerns regarding the College's approach to GDPR and any possible data breaches.

1, Introduction

i. Governors must ensure that where information is identified as personal and/or sensitive it is stored securely and destroyed or returned to the Clerk when it is no longer current.
ii. Governors will rarely receive data which is sensitive. When they do, for example if they are hearing an exclusion appeal, they will be alerted to the sensitive nature of the information by the Clerk who will also outline the appropriate procedures for the safe use and deletion of this data. See Appendix 1 for example notification.
iii. Please clarify any matters relating to personal and/or sensitive data with the DPO if you are in any doubt.
iv. Governors must not disclose any personal and/or sensitive data to any unauthorised third party (including College staff).
v. Any suspected breaches of data security must be immediately notified to the DPO.

2, Electronic records

Electronic files must be stored on an encrypted memory stick or an encrypted hard drive.

a) General Principles relating to the safe storage and use of data stored and secured electronically

i. Governors must use robust passwords on all devices used to store, process or access personal and/or sensitive data.
ii. If governors have a need to save passwords, they are encouraged to use a Google account, and use Google's 2-Step Verification,
iii. Governors must not use a public WiFi connection to access Govweb unless it is via a trusted VPN provider e.g. Avast VPN.
iv. Governors must report any suspected security incident to the Data Protection Officer (the reporting of any incidents will be treated in confidence if necessary)

b) Email

i. Governors must take particular care with the use of email, both in ensuring the recipient of any personal and/or sensitive data is authorised to receive it and that they have adopted procedures that are compliant with GDPR.
ii. Carefully consider what you send via email and to whom you send it. Wherever possible do not send personal and/or sensitive information via email, avoid copying in people without clear and good reason and consider verifying the email address before sending it.

3, Paper records

i. Wherever possible governors must store, process and access personal and/or sensitive data electronically.

ii. When governors make notes on paper containing personal and/or sensitive data for future discussion and/or processing they must securely destroy these notes once the matter has been actioned.

iii. Governors must only take a student's personal data off site if this is necessary in order to carry out their role effectively in the interests of students, for example governors may need to have access to personal and/or sensitive data when hearing appeals against exclusion. In these circumstances they must take appropriate steps to maintain the security of the data and to ensure that it is destroyed securely or returned to the Clerk when it is no longer current.

These procedures should be considered in conjunction with the following policies:

- GDPR
- Staff Code of Conduct
- Acceptable Use Policy for Staff
- Freedom of Information
- Safeguarding

Appendix 1

Example of notification from Clerk in relation to Student Exclusion Appeal information:

It is important that you keep all information relating to the Appeal securely. Electronic communication must be kept on a personal computer or laptop not accessed by others or saved on an encrypted memory stick. Paper copies should be kept securely and handed back to the Clerk at the end of the appeal hearing for secure disposal. Electronic communication should be deleted immediately after the appeal.