DATA PROTECTION POLICY

October 2024

DATA PROTECTION POLICY

1. **Rationale**
The Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR) 2018 regulate how organisations can use personal data and protect the rights of individuals with regards to the use and storage of their personal data.

Woking College recognises that it has a legal duty to secure any information it holds and to only hold information it reasonably needs to discharge its functions as an employer and education provider effectively. This policy sets out the basis on which the College will collect and use personal data either where the College collects it from individuals itself, or where it is provided to the College by third parties. It also sets out ruiles and expectations on how the College handles, uses, transfers and stores personal data.

During the course of the College's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, students, their parents, its contractors and other third parties (in a manner more fully detailed in the College's Privacy Notice). Woking College is committed to a policy of protecting the rights and privacy of individuals, including students, staff and others, in accordance with the principles of the Data Protection Act. Protecting the confidentiality and integrity of personal data is a key responsibility of all employees, trustees and contractors within the College. The College has implemented this Data Protection Policy to ensure all College personnel are aware of what they must do to ensure the correct and lawful management of personal data.

Woking College needs to process certain information about its staff, students, parents and guardians and other individuals with whom it has a relationship for various purposes such as, but not limited to:

1. The recruitment and payment of staff.
2. The administration of programmes of study and courses.
3. Student enrolment.
4. Examinations and external accreditation.
5. Recording student progress, attendance and conduct.
6. Collecting fees and making payments.
7. Complying with legal obligations to funding bodies and government departments.

Woking College is registered with the Information Commissioner's Office (ICO), which is responsible for enforcing data protection law in the UK and will typically look into individuals' complaints routinely and without cost and has various powers to take action for breaches of the law. Our data registration number is: **ZB397619.**

Data protection legislation is overruled by other legislation including safeguarding, health and safety and prevention of crime, where there is a legal requirement to share the data. The data protection legislation provides a framework which enables information to be shared for such purposes.

2. **Principles of Data Protection**
The Data Protection principles are:

a) The processing of personal data must be lawful, fair and transparent.
Woking College will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

b) The purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and must not be processed in a manner that is incompatible with the purpose for which it is collected.
Woking College will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

c) Personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.
Woking College will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this in mind. If any irrelevant data is given by individuals, it will be destroyed immediately.

d) Personal data undergoing processing must be accurate and, where necessary, kept up to date.
Woking College will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the College if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the College to ensure that any notification regarding the change is noted and acted on.

e) Personal data must be kept for no longer than is necessary for the purpose for which it is processed.
Woking College undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means Woking College will undertake a regular review of the information held and implement an updating process.

Woking College will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

f) Personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data.
Woking College will only process personal data in accordance with individuals' rights including a right to:

- be told the nature of the information the College holds and any parties to whom this may be disclosed.
- prevent processing likely to cause damage or distress.
- prevent processing for purposes of direct marketing.
- be informed about the mechanics of any automated decision taking process that will significantly affect them.
- not have significant decisions that will affect them taken solely by automated process.
- sue for compensation if they suffer damage by any contravention of the legislation.
- take action to rectify, block, erase or destroy inaccurate data.
- request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties. Woking College will ensure that all personal data is accessible only to those who have a valid
reason for using it.

Woking College will have in place appropriate security measures e.g. ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):

- keeping all personal data in a lockable cabinet with key-controlled access.
- password protecting personal data held electronically.
- archiving personal data which are then kept securely (lockable cabinet).
- placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff.
- ensuring that PC screens are not left unattended without a password protected screen-saver being used.

In addition, Woking College will put in place appropriate measures for the deletion of personal data - manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A log will be kept of the records destroyed.

This policy also applies to staff and students who process personal data 'off-site', e.g. when working at home, and in circumstances additional care must be taken regarding the security of the data.

3. **Lawful Grounds for Data Processing**

Under GDPR, there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar which constitutes consent under GDPR and the fact that it can be withdrawn by the data subject, it is considered preferable for the College to rely on other lawful grounds wherever possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests fo the College. It can be challenged by data subjects and also means the College is taking on extra responsibility for considering and protecting people's rights and interests. The College's legitimate interests are set out in its Privacy Notice, as required under GDPR.

Other lawful grounds include:

- Compliance with a legal obligation, including in connection with employment, engagement of services and diversity
- Contractual necessity, e.g to perform a contract with staff, students or parents, or the engagement of contractors
- A narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies and specific public interest grounds.

4. **Personal and Sensitive Data**

Personal Data

Personal data is any information about an individual which either identifies them or allows them to be identified in conjunction with other information that is held. It could be as simple as a name, address, date of birth, telephone number, national insurance number, recruitment information, contract details, employment references and appraisals. For students, this could also include attendance information, assessment records and exam results. Other identifiers may include student or staff ID numbers, Unique Learner Numbers, name abbreviations and IP addresses.

If it is possible to identify an individual directly from the information processed, then that information is likely to be personal data. If the individual cannot be identified by one piece of data alone, however with additional knowledge the individual can be identified, this is still classes as personal data.

Special Category Data

Special category data is more sensitive, and so needs more protection. Special category data includes:

- race;
- ethnic origin;
- political opinions and/or affiliations;
- religious beliefs;
- trade union membership;
- genetic data;
- biometric information (where used for ID purposes);
- health records;
- sex life or sexual orientation
- criminal records

5. **Data Breaches**

Definition of a Data Breach

A Personal Data Breach is an event which has caused or has the potential to cause loss or damage to an individual's information and/or Woking College's reputation.

Whilst the College takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of personal data. If this happens there will be a personal data breach and College personnel must comply with the College's data breach reporting process.

A personal data breach is defined very broadly and is effectively any failure to keep an individual's personal data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of personal data. Whilst most personal data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

There are three main types of personal data breach which are as follows:

Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, personal data such as hacking, accessing internal systems that a staff member is not authorised to access, accessing personal data stored on a lost laptop, phone or other device, people "blagging" access to personal data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong person, or disclosing information over the phone to the wrong person;

Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, personal data such as loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting personal data in error, loss of access to personal data stored on systems, inability to restore access to personal data from back up, or loss of an encryption key; and

Integrity breach - where there is an unauthorised or accidental alteration of personal data.

Data Breach Reporting

When a member of staff or student suspects a data breach, they should immediately notify the College Data Protection Officer (dpo@woking.ac.uk) with full details of the breach. If the member of staff or student has been the cause of the breach or part of a process that has led to the breach, the person should not continue with that process until investigation has completed.

The Data Protection Officer (DPO) will ensure that the following is completed by the appropriate person:

- Investigate the nature of the breach, the type of data involved and, where personal data is involved, who the subjects are and how many personal records are involved. The investigation will consider the extent of a system compromise or the sensitivity of the data involved, and a risk assessment will be conducted as to what might be the consequences of the incident; for instance whether harm could come to individuals or whether data access or ICT services could become disrupted or unavailable.
  If the breach is deemed to be minor with no harm to the data subject(s), the DPO will give appropriate feedback to the staff member who initially reported the breach. However, if the breach os deemed to be serious, the DPO will request additional information from the person reporting the breach and will consider any impact on the data subjects(s).

- If the damage/harm is minimal, the processes of the relevant College area will be reviewed and amended to prevent any futher repeat. Where necessary, additional training will be given to staff involved. For more serious issues, the DPO is likely to take written statements from staff members involved.

- Take appropriate action to prevent the breach from escalating.

- Inform those individuals without undue delay if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms. The College will not be obliged to notify the individuals affected where:
  - there are technological and organizational protection measures (e.g. encryption);
  - the Controller has taken action to eliminate the high risk; and
  - it would involve disproportionate effort – in this case they may be informed some other way e.g.by a notice in newspapers.

- Keep a record of the data breach regardless of whether the College is required to notify the Information Commissioner's Office (ICO).

- Assess whether the ICO should be notified of the breach within 72 hours of becoming aware of the breach, where feasible.

If the investigation finds a possible breach, then depending on the importance of the breach the DPO may seek advice from the ICO. The DPO reserves the right to seek the advice from the ICO on any matter that is not trivial.

If the DPO is satisfied that the integrity of the College is still intact, the breach can be dealt with internally. A review of internal procedure and process may be needed or a more detailed investigation may be carried out.

All breaches will be reported to the Senior Leadership Team (SLT).

6. **Responsibilities**

This part of the Policy identifies the Data Protection responsibilities of various members of staff and students.

Principal and Senior Leadership Team

The College Executive and SLT is committed to ensuring that the College is fully compliant with the law and best practice for handling personal information. To this end the College Executive and SLT will:

- Approve College policies & procedures for handling personal data;
- Review developments in good practice and in particular, any Codes of Practice issued by the Information Commissioner's Office having a bearing on College activities, updating College policies and procedures as appropriate;
- Allocate resources (staff time and budget) to enable the compliance of the Data Protection legislation.
- Determine the College's Records Management and Information Strategies concerning how information, including personal data, is organised, categorised, stored and retrieved.
- Ensure all College staff and students receive data protection training.
- Appoint a Data Protection Officer at SLT level.

Data Protection Officer (DPO)

The DPO will be responsible for maintaining the College's data protection system (its policies and procedures).

The DPO is responsible for ensuring:

- The College's Data Protection Registration with the ICO is maintained;
- ICO guidance, data protection legislation and GDPR is monitored;
- Recommendations are made to the Senior Leadership Team on good practice and data protection policy;
- Training, guidance, the dissemination of information and advice on any specific data protection issues is provided;
- Subject Access Requests are dealt with and responses to complaints that have a bearing on other data subjects' rights (unwarranted substantial damage or distress; direct marketing; rectifying, blocking, erasing & destroying inaccurate personal data and disputed cases of inaccuracy or other alleged breaches) are co-ordinated;
- Advice on all non-routine requests for disclosure of personal information is co-ordinated;
- Data breach processes are managed and personal data breaches are investigated in line with Data Protection legislation and General Data Protection Regulations;
- Periodic data protection audits and Data Protection Impact Assessments are undertaken;
- College policies and procedures are reviewed in line with current data protection legislation;
- The College Record of Processing Activities (RoPA) is maintained.

Responsible Managers

Personal data is processed across the breadth of the College's normal everyday activities. Good personal data handling is one aspect of what employees need to do to deliver excellent services to students and parents. The key to achieving high standards in handling personal information is recognising that the primary responsibility for complying with legislation and good practice lies with those staff and managers who are responsible for deciding how in practice personal information will be used. The line managers of departments who process personal information are the responsible managers for this policy.

Responsible managers will, in respect of their departments:

- Ensure that they are satisfied with the legality of holding the information and how it is used;
- Ensure that they have written documentation assessing & identifying legitimate grounds for processing personal data and sensitive personal data;
- Make appropriate provision for the security of both manual and computerised personal data, where held locally, (back-up, contingency plans for catastrophic failure/migration of data to new systems, access to physical environment, locked files, guidelines on processing off-site, secure disposal etc). The security arrangements for computerised personal data must comply with the College's IT Policy;
- Ensure staff only have access to data including network drives required for their role.
- Ensure that staff with access to personal data receive appropriate guidance and training covering:
    - The security arrangements for the data

    - How personal data is to be collected and recorded including approved sources
    - How consent is to be obtained where this is the ground for processing personal information
    - The information data subjects are entitled to receive under the Fair Processing Code and that application forms etc. include this information
    - Any permitted routine disclosures of the data and how to respond to other requests for disclosure;
    - Procedures for regularly reviewing personal data to check that it is adequate, accurate, up to date, not excessive and deleted when no longer needed;
- Refer any non-routine requests for disclosure to the DPO;
- Promptly inform the DPO of any requests for subject access so that they can be responded to within the appropriate time limits.
- Be aware of data subjects' rights to compensation in certain cases and their right to rectify, block, erase & destroy inaccurate personal data and inform the DPO of any complaints alleging breaches of the Act or any cases where the data subject's complaint of inaccuracy is disputed;
- Ensure that personal data is not transferred outside the EEA other than in accordance with the Act;
- Ensure that any processing of personal data that is carried out by a contractor on behalf of the College is subject to a written contract that requires the data processor to act only on instructions and makes appropriate provision for the security of the data.
- Report any suspected data breach to the DPO immediately in line with the data breach process.
- Retain and archive personal data in line with appropriate guidance and best practice.
- Undertake a Data Protection Impact Assessment (DPIA) for the introduction of any potential high-risk situation for example where a new technology system is being deployed. If the DPIA indicates high risk processing this will be discussed with the Senior Leadership Team which may result in the ICO being consulted.
- Consider privacy at the initial design stages and throughout the complete development process of new products, processes or services that involve processing personal data.

IT Services
All staff and users of personal data have some responsibility for the security of that data. IT services have an important role in ensuring the security of computerised data.

In particular they will:

- Consider privacy at the initial design stages and throughout the complete development process of new products, processes or services that involve processing personal data;
- Be responsible for advising the College on the state of technological development with regard to IT security;
- Back up data on the College's servers and IT systems;
- Implement virus detection software and measures to prevent malicious software spyware, and hacking to identify potential data breaches;
- Place restrictions on access so that individuals only have access to personal data in which they have a legitimate interest;
- Passwords must be changed in accordance with IT Policy;
- Promote and police policies for use of College systems and IT facilities including e-mail, intranet and Internets that ensure compliance with the College's Data Protection obligations and investigate breaches of IT security and report any suspected personal data breach to the DPO in line with the Data Breach process;
- Ensure all laptops have a suitable encryption method installed including two-factor authentication.

Human Relations
An important aspect of security is ensuring the reliability of staff. The People Operations team can contribute to this aim in a number of ways. They will:

- Ensure that the College's Employment Practices are consistent with the Information Commissioner's Employment Practices Code of Practice;
- Ensure that the Data Protection obligations of staff are reflected in the College's Disciplinary Procedures and contracts of employment;
- Ensure that all staff are aware of the types of personal information that the College will routinely make public (eg, name, post, academic qualifications, College telephone and e-mail) and that individuals

have the right to object to that disclosure where they consider it may cause them substantial damage or distress;
- Provide advice to responsible managers and others on the application of the pre-employment vetting process;
- Report any suspected personal data breach to the DPO in line with the data breach process.

Marketing
The Marketing Manager will ensure that consent is obtained for the purpose of marketing courses and events at Woking College, including photography and video usage.

All Staff
All staff are likely to use and have access to some personal data in the course of their duties, for example other staff, students or members of the public.They will:
- Respect the privacy and confidentiality rights of all data subjects. In particular they should be careful that personal data is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party. Unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. This includes making sure that casual access to data is not possible, (for example by members of the general public seeing computer screens or printouts).
- Only use personal data for approved purposes and ensure that they comply with any instructions and guidelines they are given about the use of personal data.
- Inform the 'Responsible Manager' of any proposed new uses of personal data.
- Keep all personal data secure and not remove it from College premises without the permission of the appropriate 'Responsible Manager'.
- Comply with all College policies regarding the use of IT facilities, e-mail and Intra/Internet.
- Ensure personal devices are encrypted and/or password protected.
- Where USB devices are used, ensure they are appropriately encrypted and/or password protected.
- Check that the information they provide to the College in connection with their employment is accurate and up to date and inform the College of changes to or errors in information held.
- Report any suspected personal data breach to the Data Protection Officer. Refer to section 3 for what is personal data.
- Contact the Data Protection Officer with any data protection queries.
- Ensure no third party is engaged to process data without written authorisation from the Senior Leadership Team.
- Not access College systems outside of the EEA (European Economic Area).
- Be responsible for access to their online live streaming sessions and recordings.
- Ensure data processed and retained is kept accurate and up to date in accordance with the Data Quality section 9.

Students
Students will not normally process personal data in the course of their studies or in other ways on behalf of the College. However, where from time to time this happens, they will need to inform their tutor and comply with the guidelines and any other instructions given to them.

At all times students will:
- Respect the privacy and confidentiality rights of all individuals.
- Not seek to use or gain unauthorised access to personal information.
- Comply with all College policies regarding the use of IT facilities, e-mail and internet/intranets.
- Check that the information they provide to the College in connection with their studies is accurate and up to date and inform the College of changes to or errors in any information held.
- Refer any data protection queries and report any suspected personal data breach to the DPO by emailing dpo@woking.ac.uk.

7. **Appointing Contractors who Access the College's Personal Data**

If the College appoints a contractor who is a processor of the College's personal data, data protection laws require that the College only appoints them where the College has carried out sufficient due diligence and only where the College has appropriate written contracts in place.

As data controller, Woking College must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both

new and existing suppliers. Once a Processor is appointed, they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

Woking College would be deemed to have appointed a Processor where another organisation is engaged to perform a service for the College and as part of it, they may have access to personal data held by the College. The College, as Controller, remains responsible for what happens to the personal data.

Woking College will ensure that any contract with a Processor contains the following obligations as a minimum:

- to only act on the written instructions of the Controller;
- to not export personal data without the Controller's instruction;
- to ensure staff are subject to confidentiality obligations;
- to take appropriate security measures;
- to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;
- to keep the personal data secure and assist the Controller to do so;
- to assist with the notification of data breaches and Data Protection Impact Assessments;
- to assist with subject access/individuals' rights;
- to delete/return all personal data as requested at the end of the contract;
- to submit to audits and provide information about the processing; and
- to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

In addition, the contract should set out:

- the subject-matter and duration of the processing;
- the nature and purpose of the processing;
- the legal basis for the processing;
- the type of personal data and categories of individuals;
- the obligations and rights of the Controller;
- the obligations and rights of the Processor;
- liability clauses to protect the College against fines associated with personal data breaches caused by the Processor.

8. **Misuse of Data**

Disciplinary action, including dismissal, may be taken against any employee who contravenes any instruction contained in, or following from, this Data Protection Policy and guidelines issued by Woking College. Upon discovering that this policy is not being complied with, or if an intentional breach of the Data Protection Principles has taken place, the Data Protection Officer in consultation with the SLT, shall have full authority to take such immediate steps as considered necessary.

9. **Retention, Archiving and Destruction**

Archiving and Destruction: Personal Data must not be kept for longer than needed

Data Protection laws require the College does not keep personal data longer than is necessary for the purpose or purposes for which the College collected it.

Data retention periods for personal data we process are detailed within the College Data Protection Retention Schedule (see Appendix 3). Further information can be provided on request by the Data Protection Officer by emailing dpo@woking.ac.uk.

If College staff feel that a particular item of personal data needs to be kept for more or less time than the retention period, for example, because there is a requirement in law or, if College staff have any questions about this policy or the College's retention practices, they should contact the Data Protection Officer.

Records for archiving should be filed in archive storage box with details of the owner and destroy date in line with the retention period listed in the Retention Schedule.

The Senior Manager for a department is responsible for maintaining a record of the data retained within the archive in line with the College data retention periods.

The Estates/Facilities department is responsible for:

- ensuring the archived records are retained in a secure, water and fireproof environment
- retrieving the archived records within 2 days of receipt of a request for the records
- confidentially destroying the records retained within the archive on the destroy date on the box.

10. **Data Quality: Ensuring the use of accurate, up to date and relevant personal data**
Data Protection Laws require that the College only collects and processes personal data to the extent that it is required for the specific purpose(s) notified to the individual in a privacy notice (see section 13) and as set out in the College's record of how it uses personal data. The College is also required to ensure that the personal data the College holds is accurate and kept up to date.

    Formal practices for the collection of up-to-date data are in place to ensure data accuracy. Checks are carried out at application and enrolment stages as well as through tutor groups. If the data is inaccurate or out of date, rectification processes are in place to ensure it is erased or rectified.

    All College staff that collect and record personal data shall ensure that it is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of personal data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. All data entry staff are trained to collect the necessary data into te College's Management Information System (MIS).

    All College staff that obtain personal data from sources outside the College shall take reasonable steps to ensure that it is recorded accurately, is up to date and limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require College staff to independently check the personal data obtained.

    In order to maintain the quality of personal data, all College staff that access it shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to personal data which the College must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

    The College recognises the importance of ensuring that personal data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection laws. Any request from an individual for the amendment, rectification, erasure or restriction of the use of their personal data should be forwarded to the Data Protection Team by email to dpo@woking.ac.uk.

    Training – All individuals who have access to personal data are appropriately trained in data protection. This is completed at point of employment at a new staff induction session and at regular intervals via both face-to-face and online training sessions. Training records are maintained by the staff development team.

11. **Data Security**
Woking College takes data security very seriously and has appropriate technical and organisational security measures in place to monitor, control and audit to protect against unlawful and unauthorised processing, accidental loss, destruction or damage to personal data. This includes, but is not limited to:
    - Multi-factor authentication
    - Email quarantine
    - Cyber Essentials accreditation
    - The use of complex passwords
    - Dark web monitoring
    - Sharing through encrypted documents or One Drive
    - Access from abroad (for staff) only temporarily and on request
    - Regular in-house 'Phishing' testing campaigns

12. **Consent as a basis for processing**
Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner. Consent is especially important when Woking College is processing any sensitive data, as defined by the legislation.

Woking College understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via the enrolment form) whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

"Personal Details
● For the purposes of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 you consent to the College holding and processing personal data including sensitive personal data of which you are the subject, details of which are specified in the College's data protection policy.
● This will include marketing images and the College CCTV."

Woking College will ensure that any forms used to gather data on an individual will contain a statement (fair collection statement) explaining the use of that data, how the data may be disclosed and also indicate whether or not the individual needs to consent to the processing.

Woking College will include the specified statement from the DfE on the student enrolment form and update when required following the ESFA's technical guidance:

How We Use Your Personal Information
This privacy notice is issued by the Education and Skills Funding Agency (ESFA), on behalf of the Secretary of State for the Department of Education (DfE). It is to inform learners how their personal information will be used by the DfE, the ESFA (an executive agency of the DfE) and any successor bodies to these organisations. For the purposes of the Data Protection Act 1998, the DfE is the data controller for personal data processed by the ESFA. Your personal information is used by the DfE to exercise its functions and to meet its statutory responsibilities, including under the Apprenticeships, Skills, Children and Learning Act 2009 and to create and maintain a unique learner number (ULN)
and a personal learning record (PLR).

Your information may be shared with third parties for education, training, employment and well-being related purposes, including for research. This will only take place where the law allows it and the sharing is in compliance with the Data Protection Act 1998.

You can opt out of contact for other purposes by ticking any of the following boxes if you do not wish to be contacted:

- *About courses or learning opportunities.*
- *For surveys and research.*
- *By post.*
- *By phone.*
- *By email.*

Further information about use of and access to your personal data, and details of organisations with whom we regularly share data are available at:
https://www.gov.uk/government/publications/esfa-privacy-notice

Woking College will ensure that if the individual does not give his/her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

13. **Transparent Processing: Privacy Statements**
The DPO will ensure that Staff and Student Privacy Statements are regularly reviewed, updated and available on the College websites and staff portals.

These set out how personal information is used and in particular:

- Why the College collects personal information
- The personal information that the College collects
- How the College collects the personal information
- How the personal information is stored
- How the College uses the personal information
- The legal basis on which the College collects and use personal information

- Who has access to personal information
- How the College shares personal information
- The transfer of personal information outside of Europe
- How the College protects personal information
- How long the College retains personal information
- An individual's rights over personal information

14. **Subject Access: Individuals' Rights**

GDPR gives individuals more control of how their data is collected and stored and what is done with it. The different types of rights are reflected below:

General Enquiries

A student or member of staff can ask the College to see information that the College holds about them by making a general enquiry to the appropriate department, such as how much they owe in fees if they are a student. The College may carry out identify checks to ensurethat they are who they say they are, but in general, the information will be disclosed to them.

Data Subject Acces Requests

An individual also has a legal right under the Data Protection Act 2018 and GDPR to be informed about whether or not any onformation is held about them and to see a copy of it. This is known as a right of subject access. Woking College students and staff have the right to:

- A copy or description of the information that the College holds about them. This information may be held electronically (for example on computer, closed circuit TV, video or audio recordings) or in paper records. The College will provide the information in an electronic format where possible. Paper records will be scanned unless the original paper copy is requested.
- The personal data will be provided in a structured, commonly used and machine-readable format unless the original paperwork is requested. Formats will include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data if required.
- The College will explain any technical terms or abbreviations so that they can understand what they mean.
- Be informed about the purpose(s) for which the information is processed.
- Be informed about the source(s) of information and recipient(s) or classes of recipients to whom the College may have disclosed the information.

Students have the right to see some exam-related information, such as marks, examiner's comments and minutes of examination appeals panels. If a student asks for exam results before they have been announced, the College will respond within 30 days from when the individual's results are published.

There may be circumstances where not all information about an individual can be provided. The DPO will ensure that, where necessary, such information will be redacted. There may be exemptions under the Act that the College needs to apply, these are:

- Crime prevention and tax collection
- Immigration control
- Required by law / legal proceedings
- Regulatory functions
- Third party data
- Management forecasts / negotiations
- Confidential references
- Exams, scripts and marks
- Safeguarding, health and safety, social work, child abuse and education records which may cause harm

Timescale

The College will endeavour to reply promptly to the request within one month, provided that the College has evidence of the individual's identity and enough information to search for the information. Where the College asks for additional information, the one-month countdown starts when the additional information has been received.

This can be extended up to a further two months where the request is complex or a number of requests have been received. Any decision in relation to wjether the request is complex will be made by the data protection officer and the College will inform the individual within one month of receipt of the request and explain why the extension is necessary.

Where the College is not taking action in response to a request, the College will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Cost
There will be no cost for a subject access request unless the request is manifestly unfounded or excessive by the data subject such as a repeated request. Where a request from a data subject is manifestly unfounded or excessive, the College may charge a reasonable fee for dealing with the request or refuse to act on the request. The fee will be determined by the cost to the College.

How to Make a Subject Access Request
Data Subject Access Requests should be emailed or sent in writing to the College Data Protection Officer (dpo@woking.ac.uk).

The individual will need to provide:

- The necessary information from the individual to confirm the individual identity. Please provide any of the following items: -
    - Birth certificate, marriage or civil partnership certificate, driving licence (photo card or paper), passport, two different utility bills (for example gas, electricity or water).
- Sufficient information from the individual to help the College locate the information that the individual has requested.

The College student or staff member should provide as much information as they can to help the College locate the information, for example how far back in time the individual would like the College to search, or providing names of members of staff who the individual has been in contact with or specific areas in the College where the individual thinks that information may be held.

The information that the individual provides will be used to manage and administer the individual's request and carry out searches for information that is held about the individual.

Requests on Behalf of Other People
An individual may make an access request on behalf of another person. The College will send them a copy of information held only with the consent and authorisation of the subject. Data Subject Access should be emailed or sent in writing to the College Data Protection Officer (dpo@woking.ac.uk).

If a parent or guardian makes a request on behalf of an individual person under 18, the College may make additional enquiries to confirm that they have parental responsibility before releasing information. This may involve discussing the request with staff members within the College and/or with relevant external agencies.

Information That Relates to Other People
Under the Data Protection Act 2018, an individual is only entitled to see information that is held about them. There may be occasions when information about other people is held on the individuals' records. The College may inform the third party that a subject access request has been made and inform them that their personal data is contained within the request. The College may contact the third party for their consent to release information that identifies or relates to them. The College is entitled to redact information about the subject if the third-party consent has been withheld or cannot be obtained.

Right of Erasure (Right to be Forgotten)
This is a limited right for individuals to request the erasure of personal data concerning them where:

- the use of the personal data is no longer necessary;
- their consent is withdrawn and there is no other legal ground for the processing;
- the individual objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data has been unlawfully processed; and
- the personal data has to be erased for compliance with a legal obligation.

In a marketing context, where personal data is collected and processed for direct marketing purposes, the individual has a right to object to or remove consent to processing at any time. Where the individual objects, the personal data must not be processed for such purposes. However, when giving consent for such purposes, individuals will be informed that it may take up to 12 months' to fully remove their information from some aspects of marketing, such as the College prospectus.

Right of Data Portability
An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine-readable format where:

- the processing is based on consent or on a contract; and
- the processing is carried out by automated means

This right isn't the same as subject access and is intended to give individuals a subset of their data.

Correction or Deletion of Inaccurate Information
On receipt of a correction or deletion of inaccurate information, the College will investigate the inaccuracy and any changes will be made within one month.

This may be extended where the request is complex or a number of requests have been received. The College will inform the individual within one month of receipt of the request and explain why the extension is necessary.

If the individual has any queries, or needs assistance with making a request, please contact the College Data Protection Officer: dpo@woking.ac.uk.

Further information
Impartial information and advice is available from the Information Commissioner's Office. The website is available at www.ico.org.uk.

15. **Disclosure of Data**
Only disclosures which have been notified under the College's DP notification must be made and therefore staff and students should exercise caution when asked to disclose personal data held on another individual or third party.

Woking College undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies and in some circumstances, the police. Legitimate disclosures may occur in the following instances:

- the individual has given their consent to the disclosure.
- the disclosure has been notified to the ICO and is in the legitimate interests of the College.
- the disclosure is required for the performance of a contract.

There are other instances when the legislation permits disclosure without the consent of the individual. For detailed duidance on disclosures, see the Code pf Practice (CoP).

Under no circumstances will Woking College sell any of its databases to a thrd party.

16. **Email**
It is the policy of Woking College to ensure that senders and recipients of email are made aware that under the DPA and Freedom of Information legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the College's email.

Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from the College may be accessed by someone other than the recipient for system management and security purposes.

17. **CCTV Images and Monitoring**
The College site has a CCTV system to prevent and detect behaviour which is in breach of the staff or student code of conduct, detects crime and safeguards all members of the College community.

The College does not use software to automatically identify individuals using biometric data. Therefore, images routinely captured and stored do not constitute personal information until this identification has taken place, but the data must be kept securely, and encrypted.

Direct access to live CCTV images is restricted only to senior managers, IT staff and the site security team. Images may be stored for up to 30 days, except where an incident has been detected where video clips or snapshots may be kept, and made available to appropriate staff, until the proceedings of any incident has been concluded.

Where an incident has been recorded, and the CCTV image has been captured in this way, it will form part of the personal information for those affected, and therefore is subject to Subject Access Requests. Images will only be released where no other identifiable person is within the image.

Where a crime has been alleged to have been committed, the College may release images to appropriate bodies as part of their investigation, such as the police or insurance companies.

18. **Marketing and Consent**

The College will sometimes contact individuals to send them marketing or to promote the College. Where the College carries out any marketing activities, it will do so in a legally compliant manner.

Marketing consists of any advertising or marketing communication that is directed to particular individuals.

Privacy and Electronic Communications Regulations (PECR) sit alongside data protection and apply to direct marketing i.e. a communication directed to particular individuals and covers any advertising/marketing material. It applies to electronic communication i.e. calls, emails and texts. PECR rules apply even if you are not processing any personal data.

Consent is central to electronic marketing and the College uses opt-in boxes as a default. The College uses a 'soft opt-in' if the following conditions are met in line with ICO guidance:

- contact details have been obtained in the course of a sale (or negotiations for a sale)
- the College are marketing its own similar services; and
- the College gives the individual a simple opportunity to opt out of the marketing, both when first collecting the details and in subsequent messages after that.

19. **Automated Decision Making and Profiling**

Woking College does not make decisions solely based on automated decision-making without any human involvement.

20. **Data Protection Impact Assessments (DPIA)**

The GDPR introduced a new requirement to carry out a risk assessment in relation to the use of personal data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment (DPIA). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using personal data but is an assessment of issues affecting personal data which need to be considered before a new product/service/process is rolled out. The process is designed to:

- describe the collection and use of personal data;
- assess its necessity and its proportionality in relation to the purposes;
- assess the risks to the rights and freedoms of individuals; and
- identify the measures to address the risks.

A DPIA must be completed where the use of personal data is likely to result in a high risk to the rights and freedoms of individuals. The College uses a standard template using the ICO's standard DPIA as a template. The College's standard format DPIA is available in Appendix 1 and from the Data Protection Officer.

Where a DPIA reveals risks, which are not appropriately mitigated the ICO must be consulted by the DPO.

Where the College is launching or proposing to adopt a new process, product or service which involves personal data, the College needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The College needs to carry out a DPIA at an early stage in the process so that the College can identify and fix problems with its proposed new process, product or service at an early stage,

reducing the associated costs and damage to reputation, which might otherwise occur.

Situations where the College may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):

- large scale and systematic use of personal data;
- entering into working contracts with other organisations where data processing will occur;
- large scale use of Special Categories of Personal Data, or personal data relating to criminal convictions and offences eg, the use of high volumes of health data; or
- systematic monitoring of public areas on a large scale eg, CCTV cameras.

All DPIAs must be reviewed and approved by the DPO.

21. **Transferring Personal Data to a Country outside the EEA**
Data Protection laws impose strict controls on personal data being transferred outside the European Economic Area (EEA). Transfer includes sending personal data outside the EEA but also includes storage of personal data or access to it outside the EEA. It needs to be thought about whenever the College appoints a supplier outside the EEA or the College appoints a supplier with group companies outside the EEA which may give access to the personal data to staff outside the EEA.

Woking College will not transfer data to such territories without the explicit consent of the individual or without the approval of the Data Protection Officer.

This also applies to publishing information on the internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA - so Woking College will always seek the consent of individuals before placing any personal data (including photographs) on its website.

22. **College Forms**
All College forms and procedures must be reviewed by the College Data Protection Officer who will assess for Data Protection Act 2018 and GDPR requirements.

Forms
All College forms must include:

- Why the College is collecting the data
- How long it is retained and that it is destroyed
- Where it is stored (electronically and paper based)
- Who has access to it
- Who it is shared with
- Your rights relating to your personal information
- Who to contact to amend/remove personal information

23. **Compliance**
This policy applies to all staff, students, trustees and contractors of Woking College. Any breach of this policy or of the regulation itself will be considered an offence and the College's disciplinary procedures may be invoked.

As a matter of best practice, other agencies and individuals working with Woking College and who have access to personal information, will be expected to read and comply with this policy. It is expected that departments who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign an agreement which, among other things, will include a statement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998 and other relevant legislation. The Code of Practice on GDPR for Woking College gives further detailed guidance and Woking College undertakes to adopt and comply with this Code of Practice.

The ICO's website (www.ico.gov.uk) provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests and how to handle requests from third parties for personal data to be disclosed. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website.

For help or advice on any data protection or freedom of information issues relating to Woking College, please do not hesitate to contact: The Data Protection Officer (DPO) by emailing dpo@woking.ac.uk.

24. **Glossary of Terms**

College – Woking College, Rydens Way, Woking, Surrey. GU22 9DL.

College Personnel – Any College employee, worker or contractor who accesses any of the College's personal data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.

Data - Data is information, which is processed automatically (by a computer), or is manual data which forms part of a relevant filing system. A relevant filing system is a system that is structured either by reference to an individual or by criteria relating to individuals so that specific details relating to a particular individual may be easily selected from that system. Data can be written information, photographs, or information such as fingerprints or voice recordings.

The Freedom of Information Act extends the definition of data to include unstructured manual data that is held for personnel purposes - where employees request access to their own personal data.

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

Data Controller – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use personal data. Woking College is a Data Controller.

A Controller is responsible for compliance with Data Protection laws. Examples of personal data the College is the Controller of include employee details or information the College collects relating to students. The College will be viewed as a Controller of personal data if it decides what personal data the College is going to collect and how it will use it. A common misconception is that individuals within organisations are the Controllers. This is not the case as it is the organisation itself which is the Controller.

Data Processor – Any entity (eg, company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller.

A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include: where software support for a system, which contains Personal Data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services.

Data Protection Laws – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

Data Protection Officer – The College Data Protection Officer is the Deputy Principal.

Data Subject - The Data Subject is the individual who is the subject of personal data. This will include staff, students, suppliers of goods and services etc.

EEA – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden. Note – From 31st January 2020, the UK is no longer a member of the EEA or EU.

ICO – the Information Commissioner's Office, the UK's Data Protection regulator.

Individuals – Living individuals who can be identified, *directly or indirectly*, from information that the College has. For example, an individual could be identified directly by name, or indirectly by gender, job role and

office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students.

Personal Data – Any information about an individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held.

Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of individuals in companies such as firstname.surname@ organisation.com) and IP addresses. Personal data also includes any other form of identifier such as unique ID numbers, initials and job titles as well as more sensitive types of data such as trade union membership, genetic data and religious beliefs. These more sensitive types of data are called "Special Categories of Personal Data" and are defined below. Special Categories of Personal Data are given extra protection by Data Protection laws.

Processing - Is anything done with the data including holding and viewing data. It includes

obtaining	reading and consulting
holding	disclosing
amending	transferring
collating and compiling	blocking, deleting or destroying information

If the individual has personal data in the individual's possession, the individual should assume that the individual is processing it.

Special Categories of Personal Data – Personal data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (ie, information about their inherited or acquired genetic characteristics), biometric data (ie, information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary personal data.

Third Party - Is any person other than the data subject, the data controller, the data processor or other person authorised to process data for the data controller.

If you require any further information or have any questions or queries relating to this document, please contact the Data Protection Officer: dpo@woking.ac.uk.

Were changes made to the Policy when received? If YES complete the Partial Equality Analysis table.

Questions for all Policies Is it likely that the Policy Revision could have a negative impact:-	Please Tick Box YES	 NO
On minority ethnic groups?		X
Due to gender?		X
Due to disability?		X
Due to sexual orientation?		X
Due to their religious beliefs (or none)?		X
On people due to them being transgender or transsexual?		X
Additional questions for Policies relating to Staff Is it likely that the Policy Revision could have a negative impact:-		
On people due to their age?		X
On people due to their marital or civil partnership status?		X
On people with dependants/caring responsibilities?		X

Date of Review	October 2024	Did you make changes?	Yes	

If YES please speak with The Assistant Principal as a full Equality Analysis may be required.

Appendix 1:

Data Protection Impact Assessment Form

This form should be completed at the start of any major project involving the use of personal data or if you are making a significant change to an existing process. The final outcomes should be integrated back into the project plan.

Name of proposer	
Title of project or proposal	
1. Identify the need for a DPIA	Explain broadly what the project aims to achieve and what type of processing it involves. Summarise why you identified the need for a DPIA.
2. Describe the processing	**Describe the nature of the processing**: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? What types of processing identified as likely **high risk** are involved?
	Describe the scope of the processing: what is the nature of the data and does it include **special category** data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
	Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would thye expect you to use their data in this way? Do they include children and other vulnerable groups? Are there any prior concerns over this type of processing or security flaws?
	Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for the College, for the students and more broadly?
3. Consultation process	Describe when and how you will consult with relevant stakeholders or justify why its not important to do so. Who else do you need to involve in the College? Do you need to ask any processors to assist? Do you plan to consult with data security experts?

4. Assess necessity and proportionality	Describe compliance and proportionality measures in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you ensure data quality and data minimisation? What information will you gve individuals? How will you help to support their rights? What measures will you take to ensure processors comply? How do you safeguard any international transfers?				
5. Identify and assess risks	Describe the source of risk and nature of potential impact on individuals, including associated compliance and corporate risks as necessary		Likelihood of harm	Severity of harm	Overall risk
			Remote, possible or probable	Minimal, significant or severe	Low, medium or high
6. Identify measures to reduce risk	Risk	How to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
			Eliminated, reduced or accepted	Low, medium or high	Yes/No
7. Recorded outcomes	Item	Name/Position/Date	Notes		
	Measures approved by: Originator and SLT manager				
	Risks approved by: Data Protection Officer				
	Summary of DPO advice:		DPO advice accepted or overruled? If overruled, explain your reasons		
	Consultation responses reviewed by:		Emerging issues from consultation:		

Data Protection Impact Assessment accepted:		**Name**	**Signature and date**
	Project proposer		
	Project Sponsor (SLT)		
	Data Protection Officer		

Appendix 2a: Data Protection Privacy Notices

Woking College Privacy Notice – Staff (including applicants and volunteers) and Trustees

How we will use your personal information?

Woking College is a 16-19 Sixth Form College Academy Trust based in Woking, Surrey, specialising in education for Sixth Form students. You can find more about us at www.woking.ac.uk. Woking College is registered with the Information Commissioner's Office (ICO) where the purposes for which the College collects and processes personal data are notified.

Your data and privacy is of upmost importance to us and we are committed to keeping your personal data safe. This notice will help you to understand how we collect, use and process your personal data.

The College will collect, store and process your personal data only for the legitimate interest of administering the College and the execution of the College's Public Task of providing education on behalf of the Government. This includes what you disclose on your application, at interview and what is learnt about you afterwards as a staff member, trustee or volunteer.

The College requires certain information about you in order to administer your position as a member of staff, or applicant to be a member of staff, trustee or volunteer at the College. In particular the College will collect and process:

- Your contact details, any information you provide on your application including previous employer details, and the results of any reference request in order to administer the appointment process.
- Certain classes of sensitive personal information only for the purposes of statistical monitoring of Equality and Diversity of the workforce.
- Information relevant to 'Keeping Children Safe in Education', School Staffing Regulations (2013), or 'Section 128' checks relevant to your role.

This information will only be kept for 6 months after the interview date for applicants who are not appointed, unless otherwise agreed.

For members of staff and trustees, the information that we may collect are as follows:

- **Basic personal details** such as your name, initials, date of birth and position held.
- **Personnel information** such as your contact details, gender, nationality, attendance records, proof of ID and qualifications, training and professional review records, education and employment history, information needed to perform your DBS check, and medical records where they relate to your attendance at College, and to monitor the College's performance on equality.
- **Financial information** such as salary records, bank details, income tax and NI records and pension records as well as any other details needed to operate the Payroll service.
- Your **photo image and car registration details**, in order to operate the College ID Card system and enable members of the College to identify you or your vehicle as a member of staff.
- Information about **your performance** in relation to your employment in your role, such as Professional Reviews, lesson observations and exam results of the students you have taught.
- Information about your use of the **Cashless Catering** system.
- **Health and Safety records** relating to the COSHH regulations (use of chemicals)
- **Marketing Information** including work-related photos of you and information about your time at the College. Your consent will be sought separately before using such information.

- If you take part in **Trips and Visits** we may collect information such as your passport details, additional medical information and details of your travel insurance.
- **CCTV footage** will be captured of you when you are on the College campus. The College is equipped with a CCTV system for the purpose of the security and safeguarding of College members and visitors and the detection of crime. The CCTV images will not be used for any other purpose.

Who we share your information with the following third parties:

- The College's appointed Payroll and Pension Services providers
- Disclosure and Barring service and other regulatory agencies
- The S7 Consortium and other training providers where you may be asked to participate
- The College's HR consultants and, where necessary, our Occupational Health Provider
- Credit Reference Agencies who have made an enquiry on your behalf
- Future employers in respect of references where you have given consent

Third parties acting our behalf such as:

- IT services – Microsoft, online teaching services and companies that provide online resources
- Auditors, acting on behalf of the Board of Trustees or the ESFA
- Courts, law enforcement agencies and other emergency services as necessary to comply with a legal requirement, for the administration of justice, to protect vital interest (to prevent death or serious harm), to protect the security or integrity of College operations, and to detect, investigate or prevent crime.
- Travel agents, airlines and other companies with which you have engaged with to organise a College Trip

Access to your information

You have a right to request the information we hold about you. 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, unless there is a good reason for the delay – in this case you will be informed about the reason for the delay.

If an individual makes a request which is deemed to be excessive or unfounded, the College may charge a fee commensurate with the cost, or refuse to provide the information requested.

Transferring your data

Any data that is shared will be subject to the Data Protection Act (2018).

Correcting mistakes

You have the right to request we update any information we hold about you if you think it is incorrect, incomplete or out of date. If we believe the information we hold about you is correct we may refuse to update our records but we will note your objection.

Objecting to how we process your data

We have a legitimate interest in processing your personal information in relation to the Public Task of the College business. You have the right to object, on grounds relating to your particular situation, to us processing your personal data where you feel the processing has a disproportionate impact on your rights and is in excess of this legal basis.

Automated processing

We do not carry out any automated processing.

The right to be forgotten

You can ask us to erase your personal data in the following situations:

- The data is no longer necessary in relation to the purpose for which it was originally collected
- You have objected to us processing the data and there is no overriding legitimate interest for us to continue the processing
- Your personal data was unlawfully processed
- Your personal data has to be erased in order to comply with a legal obligation

We may in some circumstances refuse to erase your personal data. If we do this we will explain why and the legal reason for doing so.

Your rights

If you have any questions or queries about the information we hold about you, and how we use it, you can either speak to your Line Manager or Clerk of the Academy Trust. Alternatively, you can address your concerns to the College's Data Protection Officer, who can be contacted via email: dpo@woking.ac.uk.

If you feel your question or complaint has not been addressed to your satisfaction, you can contact the:

Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow.
SK9 5AF.

This statement will be subject to regular review and will be updated accordingly.

Appendix 2b: Data Protection Privacy Notices

Woking College Privacy Notice - Students

How we will use your personal information?

Woking College is a 16-19 Sixth Form College Academy Trust based in Woking, Surrey, specialising in education for Sixth Form students. You can find more about us at www.woking.ac.uk. Woking College is registered with the Information Commissioner's Office (ICO) where the purposes for which the College collects and processes personal data are notified.

Your data and privacy is of upmost importance to us and we are committed to keeping your personal data safe. This notice will help you to understand how we collect, use and process your personal data. You may wish to show this to your parents/carers to help you fully understand it.

In order to administer your place at Woking College, we collect information from you and about you in various ways including via your original application as well as from your school, references, enrolment and interviews, attendance data, the College CCTV system, University and College Admissions Service (UCAS), exam boards as well as your interactions with your teachers, parents, and tutors at College. The College has strict policies on what information we hold, how it can be used and when it must be destroyed. You can see your own personal information via the Student Portal or by speaking to your Personal Tutor.

The information we hold about you may include 'Special Category' information, such as learning needs in order to provide support for your learning and administer special exam arrangements, or ethnicity, gender or health information for the purpose of monitoring the Equality and Diversity of the College as a whole. This information will be kept especially carefully and accessible only to those specifically authorized.

We will use your information to communicate with you and your parents to inform about your progress and attendance. This is the normal operation of College systems designed to ensure you perform to your potential. If you have any concerns about this, please speak to your personal tutor in the first instance.

Your information will be passed to various Government and other agencies including the Department for Education and its related agencies (such as the Education and Skills Funding Agency (ESFA)), Learner Records Service, Examination Boards, UCAS as well as organisations such as those which provide results and performance analysis for the College. It is the legal duty of the College to communicate with these agencies in the execution of its Public Task.

In some specific circumstances, it may be necessary to perform a criminal records check with the Disclosure and Barring Service, such as where you apply to perform work experience that involves working with children.

The school you attended before enrolling at the College, along with your Local Authority, has a duty to monitor the progression of its pupils after Year 11; we may inform them that you have applied and the progress of your application – up to and including your final exam results and your destination after College (e.g. university). This information will not be released to the public without your consent.

You school is also required to provide us with any safeguarding information they hold about you, and similarly, we are required to pass on any safeguarding information to any institution you attend should you leave the College before your 18th birthday.

All these organisations have their own Data Protection policies and are all regulated and monitored by the Information Commissioner's Office.

We treat your personal information with respect: it will only be available to authorised people and organisations, not used for commercial gain and will be destroyed when it is no longer needed. Unauthorised access (or attempts to access) of personal data contravene the College's Data Protection Policy. For more information about Data Protection and how long we keep your data, please consult the College Data Protection Policy, which is available on the website.

We may also provide your information to the police, medical personnel or any other official where we believe it is in your vital interests, or in that of others, and that to withhold it would be detrimental.

Publicity

We will not disclose your personal information for publicity purposes without your express permission.

Alumni

Separately from your official 'Destination' (which is required to perform the College's Legal Duty), when you leave College, you may be invited to join the College Alumni programme, which is intended to keep you abreast of developments at College, track your progress and invite you to participate in helping future students. Joining the Alumni programme is with your consent, your information will not be shared outside the College or used for publicity without your express permission. You may remove your consent and ask for your information to be corrected or erased.

Correcting mistakes

You have the right to request that we update any information we hold about you if you think it is incorrect, incomplete or out of date, and we ask you to inform us if any of your personal information changes. If we believe the information we hold about you is correct we may refuse to update our records but we will note your objection. You can see the information we hold about you on you Student Portal or by speaking to your Personal Tutor.

Objecting to how we process your data

The College performs a public task on behalf of the Government, and therefore has a legal obligation to process your information and retain it in accordance with our policies. You have the right to object, on grounds relating to your particular situation, to us processing your personal data where you feel the processing has a disproportionate impact on your rights.

Further information regarding these rights can be found through the Information Commissioner's Office – www.ico.gov.uk.

Complaints
If you have any questions or queries about the information we hold about you, and how we use it, you can speak to your Personal Tutor in the first instance. If you still have concerns please address them to the College's Data Protection Officer. They can be contacted via email: dpo@woking.ac.uk.

If you feel your question or complaint has not been addressed to your satisfaction, you can contact the

Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow.
SK9 5AF.

This statement will be subject to regular review and will be updated accordingly.

Appendix 2c: Data Protection Privacy Notices

Woking College Privacy Notice – Parents/Carers

How we will use your personal information?

Woking College is a 16-19 Sixth Form College Academy Trust based in Woking, Surrey, specialising in education for Sixth Form students. You can find more about us at www.woking.ac.uk. Woking College is registered with the Information Commissioner's Office (ICO) where the purposes for which the College collects and processes personal data are notified.

Your data and privacy is of upmost importance to us and we are committed to keeping your personal data safe. This notice will help you to understand how we collect, use and process your personal data.

We have been provided your details by a student or applicant in relation to their application to study at Woking College. They have given your details as their nominated parent or carer, with whom we will communicate to support their studies. The student has been provided with a separate statement that you might wish to discuss with them. This includes information relating to how we will share their information with you.

In the course of the students' studies, we will collect information about you through the application and enrolment process, correspondence, and the record of any payments you have made to the College. This will be used to support the student's academic progress. We do not retain credit/debit card details.

We will keep you informed of the students' progress and of activities at the College which may be relevant to their current or future studies, such as extra-curricular activities, trips, useful resources, etc.… We will provide access for you to the 'Student Portal' through which you can monitor attendance, timetables and performance information provided by teachers.

You have the right to confirm what data we hold about you but parents and carers are not entitled to make a subject access request for data on behalf a student.

Correcting mistakes
You have the right to request we update any information we hold about you if you think it is incorrect, incomplete or out of date. If we believe the information we hold about you is correct we may refuse to update our records but we will note your objection.

Objecting to how we process your data
The College performs a Public Task in providing education on behalf of the Government, it is in performing this role that we collect and process your information. We are required to maintain emergency contact details provided by the student.

If you wish to be removed from our database, we will delete your contact information and cease communication with you. Should you subsequently wish to resume contact with the College in relation to a particular student, the student should make this request the Student Receptionist.

We are unable to provide information about any student unless the student has provided your details as their parent or carer. For more information about Data Protection and how long we keep your data, please consult the College Data Protection Policy, which is available on the website – www.woking.ac.uk.

Withdrawing consent
We do not rely on consent as a lawful basis for processing any of your information. If you choose not to give us your personal information, it may delay or prevent us from providing information relating to your son or

daughter's education. We may in some circumstances refuse to erase your personal data. If we do this we will explain why and the legal reason for doing so.

Further information regarding these rights can be found through the Information Commissioner's Office – www.ico.gov.uk.

Questions and Complaints
If you have any questions or queries about the information we hold about you, and how we use it, the please contact the College's Data Protection Officer. They can be contacted via email: dpo@woking.ac.uk.

If you feel your question or complaint has not been addressed to your satisfaction, you can contact the

Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow.
SK9 5AF.

This statement will be subject to regular review and will be updated accordingly.

Appendix 2d: Data Protection Privacy Notices

Online Applications: Privacy Statement

Information you enter onto the Woking College Online Application system will be stored securely in order to facilitate the completion of your application. You should obtain the permission of your parents/carers to provide us with their contact details before entering them on the online form. Prior to submitting your application, your information will be used only for the purposes of monitoring statistics and for you to retrieve you application details. We may contact you to offer assistance but will not use the information for marketing.

The online application information will be kept for 2 years before it is deleted from our database, during which you can view your information at any time by logging into the system. If you wish for your information to be deleted before this time, please contact the College Admissions Officer.

When you have completed the form, but before you submit your application, you will be asked to read the full 'Privacy Statement for Students' and confirm that you understand it. This notice explains how we will manage your personal data once you have applied, including our legal duties to other organisations. We will not be able to process your application unless you confirm that you have read and understood this.

If you have any questions about this, or how we will use any information you provide to us, you can contact the College's Data Protection Officer dpo@woking.ac.uk. A copy of the College Data Protection Policy can be found on the College website at www.woking.ac.uk.

Data Protection Privacy Notice – Visitors

All visitors to the College are required to sign-in, providing the name of their host and, where applicable, their vehicle registration number. A confirmation is required that the visitor has seen the notice posted on the signing-in system regarding the purpose of this data collection. This information is only available to the Administration Team and site security staff, unless a concern has been raised, for the purpose of investigation.

This information is required in order to fulfil the College's legal duty with regard to the safeguarding of young people, and the duty of care to the individual, and will be kept for a maximum of three months, unless an incident is reported under these regulations.

The College has a campus-wide CCTV system where the image of visitors will be recorded for the purpose of the detection of breach of College policies.

Data Protection Privacy Notice – Lettings

Personal information provided in relation to the letting of any College facility outside of its normal operating hours will be stored by the Director of Finance and Estates and only used in relation to the operation of the booking.

These details will serve as the point-of-contact for the purpose of safeguarding of young people and the duty of care in relation to the use of the facility and will be retained for one year after the last booking using these details.

Financial records pertaining to external bookings will be retained in accordance with current tax guidance, which is normally 7 years after the end of the relevant financial year.

The College has a campus-wide CCTV system where the image of visitors will be recorded for the purpose of the detection of breach of College policies.

Appendix 2e: Data Protection Privacy Notices

How your personal information is used by Woking College

Personal Information Type* *This list is not exhaustive*	**Description**	**Reasons for requesting Personal Data which lie within business and legitimate interests and legal duties*** *This list is not exhaustive*
Contact	Your name, date of birth, where you live and how to contact you e.g., home and mobile phone numbers ***Applies to: Students, Staff, Volunteers, Trustees, Parents/Carers***	There are a number of business and legitimate reasons it is necessary to contact you or for us to hold this information for example the Statutory Register for Trustees or emergency parental contact information. This information will be held securely and not shared with anyone else or made public. Some internal email groups will be created in which you will be able to see other members' email addresses
Contractual	Details about your employee contract or enrolment contract, including qualifications and references ***Applies to: Students, Staff*** Current employment, appointments (voluntary or other) membership of professional bodies, groups or organisations, or any other interests not mentioned above ***Applies to: Trustees***	To manage employee/employer relationships. To manage student/teacher relationships. Fulfilling contractual obligations is a legal duty. For governors we collect this information to identify possible conflicts of interest. The ESFA requires the personal contact details of the Chair of Trustees.
Locational	Data we get about where you are, such as may come from your mobile phone, the address where you connect a computer to the internet ***Applies to: Students, Staff, Volunteers, Trustees***	Complying with regulations that apply to us, for example, Data Protection and Safeguarding. See Acceptable Use of Computers Agreement.
Technical	Details on the devices and technology you use via the College WiFi ***Applies to: Students, Staff, Volunteers, Trustees***	Complying with regulations that apply to us for example Data Protection and Safeguarding. See Acceptable Use of Computers Agreement. Also monitoring business needs and where we may require additional resources.
Special types of personal data	The law and other regulations treat some types of personal information as special. We will only collect and use these types of data if the law allows us to do so: racial or ethnic origin, gender, religious or philosophical beliefs, trade union membership, genetic and bio-metric data, health data, criminal convictions and offences ***Applies to: Students, Staff, Volunteers, Trustees***	We need to collect data on learning and health needs in order to support students effectively in their studies and personal wellbeing. In order to monitor diversity effectively, it is necessary to collect personal information across all nine of the protected characteristics under the Equality Act 2010. You may be asked to complete an Equal Opportunities Form, although completion is voluntary. An annual Equality Duty report is produced and published, with all details anonymised.

Socio-Demographic	This includes details about your work or profession, nationality, education and where you/parent/guardian fit into general social or income groupings ***Applies to: Students, Staff, Trustees***	See 'Special Types of Personal Data' above. The ESFA requires this information for funding purposes. UCAS requests this information for monitoring diversity and inclusion and in making decisions related to contextual offers. We may require evidence of family income or benefits to assess your eligibility for fee remission, a bursary or free College meals.
Financial	Your bank details. ***Applies to: Staff, Volunteers, Trustees, Parents, Students***	This may be to pay staff salaries or reimburse expenses or to make bursary payments to students. Parents can provide bank details for refunds, for example, for a trip which is no longer taking place after a deposit has been paid.
Transactional	Details about payments to and from your accounts with us, and salary payments ***Applies to: Staff, Volunteers, Trustees, Parents*** Details about educational progress ***Applies to: Students*** Details about professional progress ***Applies to: Staff***	This may be to pay staff salaries or reimburse expenses or to make bursary payments to students. The College also has a legal duty to make additional employer payments relating to salary, for example, National Insurance Contributions and pension contributions through LGPS and TPS. We share this information between staff to monitor students' progress and for the purposes of report and reference writing. We share this information between line managers for the purposes of monitoring professional progress (appraisal and more widely performance management) and for the purposes of reference writing.
Documentary Data	Details about you that are stored in documents in different formats, or copies of them. This could include things like your passport, driver's licence, birth certificate or qualification certificates. ***Applies to: Students, Staff, Volunteers, Trustees***	We collect this information to ensure you are suitably qualified and have the residency status to study the course on which you are enrolled or to take up the job role for which you have been employed. For staff, this information is included on the Single Central Record for the whole period you are employed by the College.
Consent	Any permissions, consents or preferences that you give us. This includes things like permitting parents/guardians access to selected areas of your information, appointments, progress, subject reviews and/or attendance data. ***Applies to: Students***	We request this information from students in order that we can communicate effectively with parent/s and carer/s about a student's academic progress and personal wellbeing.
Open Data and Public Records	Details about you that are in public records, such as the Electoral Register, and information about you that is openly available on the internet ***Applies to: Students, Staff, Volunteers, Trustees***	Public interest. We may store this information if you work with us in a voluntary capacity or as a trustee in order to inform how we can best make use of your skills and experience.

National Identifier	A number or code given to you by a government agency to identify who you are, such as a National Insurance number or Unique Learner Number. ***Applies to: Students, Staff, Volunteers, Trustees***	We need National Insurance Numbers for legal reasons and ULNs for the efficient management of students' qualifications and examination entries.
Social Relationships	Your family, friends and other relationships ***Applies to: Students and Staff***	We sometimes request this information from you to support wellbeing or for advertising and marketing purposes. We will request your consent for this information.

Appendix 3: Data Retention Schedule (Summary)

Type of Record	Retention Period	Reason
Staff Records		
Personnel records inc. wages/salary records.	7 years from the end of employment (unless redundancy is involved, see below), or until required for the purpose of administering the College pension provision (whichever is later)	Provision of references and limitation period for litigation. Taxes Management Act 1970 Management of the College's pension provision
Staff record of an investigation where concerns were raised about their behaviour around children (even if proven unfounded) and is not malicious	Until the retirement age of the individual, or 10 years, whichever is longest.	Safeguarding[1]
Staff record of an investigation where the allegation is malicious	Not retained	
Staff application form and interview notes	6 months from date of interview date for unsuccessful candidates. Application form retained with personnel file for successful application.	Limitation period for litigation
Facts relating to redundancies	7 years from date of redundancies	Limitation period for litigation
Accident records	3 years after academic year to which the records relate	Management of Health and Safety
Records arising from health surveillance (HSE), or where a member of staff is suspected of exposure to a regulated substance	40 years in the case of exposure to carcinogens or other defined substances, otherwise 7 years after the end of employment.	COSHH regulations[2]
Trustee Records, including contract details, register of interest etc	7 years after the end of the engagement	Provision of limitation and litigation
Student Records		
Student Files, Performance Data, References etc	6 years from the end of the academic year to which the records relate	Subject access, job/education references. Audit evidence for funding and performance data.
Virtual Learning Environment records	Within the current academic year only	Operation of online learning environment
Computer usage logs/internet history	One year	To ensure the College can comply with Prevent legislation
Catering records	3 months after leaving College	To manage the catering service
Records of counselling records held on the College site	These records are not retained	Not relevant
Basic student information sufficient only to confirm whether a student attended the College.	10 years from the end of the academic year to which the records relate – in electronic form only.	Provision of limited references for ex- students.
Personal information relating to a student where a Safeguarding concern has been raised	Until the academic year following the individual's 25th birthday or 6 years after the latest contact with the student, whichever is the latest	Sector guidelines, based on the Children Act 2004.
CCTV images	30 days unless a specific incident has occurred or the images have been identified as evidence for police intervention.	Investigation of alleged or suspected criminal activity or investigation of behaviour by students which contravenes policies relating to student behaviour

[1] Child protection records retention and storage guidance | NSPCC Learning – retrieved 07 June 2021

[2] Control of substances hazardous to health (COSHH). The Control of Substances Hazardous to Health Regulations 2002 (as amended). Approved Code of Practice and guidance L5 (hse.gov.uk) – retrieved 07 June 2021