

Woodhouse College

Data Protection Policy

Approved by	Audit Committee
Approval Date	18 November 2019
Review Date	November 2022

Introduction

The College needs to keep certain information about students, staff, governors and other stakeholders to allow it to deliver teaching and learning, monitor student progress, performance, achievements, and ensure the health and safety of its staff and students. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be used fairly, stored safely and not disclosed to any other person unlawfully. In line with article 5 of the General Data Protection Regulation (GDPR), the College will comply with the following data protection principles and will ensure that personal information is:

- Processed in a lawful, fair and transparent manner;
- Collected for a specified and legitimate purpose – and not processed in a manner which is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;
- Processed in a manner that ensures appropriate security of the personal data.

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

Notification of Data Held and Processed

All staff, students, governors and other users are entitled to know

- what information the College holds and processes about them and why;
- how to gain access to it;
- how to keep it up to date;
- what the College is doing to comply with its obligations under GDPR.

The College will update staff data as and when necessary. Students' data are updated annually through the enrolment process and as necessary due to individual circumstances.

Responsibilities of Staff

All staff are responsible for maintaining the data held by the College about them and its students.

All staff are responsible for checking that any information that they provide to the College in connection with their employment is accurate and up to date. Staff must also inform the College of any errors or changes e.g., changes of address or contact numbers. The College cannot be held responsible for any errors unless the staff member has informed the College of them.

If and when, as part of their responsibilities, staff collect information about other people, (e.g., about students' work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the College procedures and guidance.

Data Security

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Personal information should be:

- kept on the College network including college OneDrives, and not stored on hard drives of PCs, laptops or other devices including memory sticks, or
- kept in a locked filing cabinet, or
- in a locked drawer, or
- in a private office, or
- if it is electronic, be password-protected.

Computers where personal data can be accessed must be logged off or locked (password enabled) when the user is not in attendance.

Staff should note that Data Protection compliance is ultimately the responsibility of all College staff. Individuals can be held legally responsible if they disclose personal information to any unauthorised third party. Breaches of data protection rules are considered to be a disciplinary matter, and may be considered gross misconduct in some cases.

In the event of an actual or a suspected data breach, staff should follow the procedure in Appendix 1.

Data Sharing

The College only shares personal data with organisations who have implemented data protection policies in line with GDPR guidance. Where the College uses proprietary software subscriptions to process personal data on its behalf, it requires them to do so on the basis of written instructions, be under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Student Obligations

Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes of address, etc., are reported to the Main Office or via Woodle.

If students using the College network process any personal data, they must ensure that they comply with the College policy and the requirements of GDPR.

The lawful basis on which we use this information

The College collects personal data under GDPR Article 6c (Legal Obligation), and 6e (Public Task) in order to meet its legal obligations with the ESFA. They are also necessary in order to carry out the public task to provide education and training. Details on the categories of data collected and who this is shared with can be found in the privacy notices for students staff and governors (Appendices 2-5).

Retention of Data

The College will retain student applicant data for one year after the application process has finished so that it can effectively deal with re-applications.

Information about students will be retained for a maximum of six years after they leave the College so that a reference can be provided or to confirm enrolment status for other reasons. As such, references cannot be provided for students who have left the College more than six years ago.

The College will retain staff applicant data for six months after the application process has finished so that it can effectively deal with re-applications.

Information about staff will be retained for the duration of their employment and for six years after they leave the College.

Examination Marks

Students will be entitled to information about their marks for both coursework and non-examination assessments. In line with the retention policy, past examination information will be available for six years after students leave the College.

Rights to Access Information

Students, parents, staff, governors and other users of the College have the right to access any personal data that is kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the college "Subject Access Request" form (Appendix 5) and submit it to the College Data Protection Officer. (Completion of this form is not mandatory but doing so will accelerate a request)

The College may charge a fee if the request is manifestly unfounded or excessive.

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 good reason for delay. In such cases, the reason for delay will be explained in writing to the person making the request.

The Right to be Forgotten

Students, parents, staff, governors and other users of the College have the right to obtain the erasure of personal data where this data is no longer necessary in relation to the purposes for which they were collected and processed. However, there are certain limits on this right, such as the need to retain data for funding or safeguarding and obligations.

Any person who wishes to exercise this right should complete the college "Subject Access Request" form (see Appendix 5) and submit it to the College Data Protection Officer. (Completion of this form is not mandatory but doing so will accelerate a request)

The College may charge a fee if the request is manifestly unfounded or excessive.

The College aims to comply with requests as quickly as possible, but will ensure that it is provided within one month unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the person making the request.

The Data Controller and the Designated Data Controller(s)

The College is the Data Controller under GDPR, and the Board of Governors is therefore ultimately responsible for implementation of this policy. However, the designated Data Protection Officer will deal with day-to-day matters.

Public Register of Data Controllers and Notification

The College has a valid notification in the data protection register that relates to processing information. This can be viewed at <https://ico.org.uk>. It is the responsibility of the Data Protection Officer to ensure the registration is checked and updated on a regular basis.

Registration Number: Z6692444
Annual Registration: April
Data Controller: Woodhouse Sixth Form College

Data Protection Officer

The nominated Data Protection Officer at Woodhouse Sixth Form College is:

Beth Yap
Data Protection Officer
Woodhouse College
Woodhouse Road
Finchley
London N12 9EY

020 8445 1210
DPO@woodhouse.ac.uk

Conclusion

Compliance with GDPR is the responsibility of all members of the College. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated College Data Protection Officer.

Privacy Notice for Students

How we use student information

Woodhouse College uses your personal information in order to provide you with courses and wider opportunities. When you are an applicant, this is necessary to communicate with you in the consideration of offering you a place at college. When you are a student, this is necessary so that it is clear what courses you are taking, to provide you with a timetable and a personal tutor, to contact you when we need to, to monitor and advise about your progress, to enter you for the right exams, to carry out our safeguarding duties and offer you the chance to participate safely in a wide range of other activities. All of these activities require that we hold your personal data and this notice gives you more information about how and why we do this.

This notice gives you more information about how the College collects, stores, processes and shares your data.

The categories of student information that we collect, hold and share include:

- Personal information (such as your name, student ID, date of birth and address), emergency contact information, your ULN and UCI numbers
- A photograph of you for identification purposes of enrolled students
- Your personal characteristics (such as ethnicity, gender, nationality and free school meal eligibility)
- Your educational achievements (such as your GCSE results) before you started at the College and your reference if your school supplied one
- Medical, financial, safeguarding and other information about support you need which help us look after you while at College
- Any additional learning needs you may have
- The courses you have taken and are taking with us
- Assessment grades and report data on enrolled classes
- Attendance information (such as the lessons you have attended and your absences and punctuality record) on enrolled classes
- The books and other resources you borrow from the College during your course
- Your exam entries and your results in external exams taken at College
- What you tell us about your wider career related experiences and ambitions
- Further photographs or information your volunteer to us which help us to communicate the work of the College and for marketing purposes
- Your academic, pastoral and behavioural record if there are problems or issues while you are enrolled in College
- Any applications you make via the College such as UCAS and any references we provide for you
- Feedback you give us about the College or, from time to time, your views on other things.
- Work experience and other references we receive about you.

Why we collect and use this information

We use your data during the application process:

- to identify and communicate with you
- to obtain a reference from your school
- to offer you a programme of A level subjects
- to gather medical and educational needs so we can support you if offered a place

We use your data when you have enrolled as a student:

- to identify you and keep the College safe
- to support your learning
- to give you a timetable
- to monitor and report on your progress
- to provide appropriate pastoral care and other support you may need
- to enter you for exams
- to request exam access arrangements or support during exams if necessary
- to enable you to make online payments and use the canteen
- to complete references and advise you about your progression options
- to assess the quality of our teaching, pastoral and other services
- to apply for funding and comply with funding agency requirements.

The lawful basis on which we use this information

We collect the following personal data under GDPR Article 6c (Legal Obligation), and 6e (Public Task) in order to meet our legal obligations with the ESFA. They are also necessary in order for us to carry out our public task to provide education and training.

- Details about yourself including your name, date of birth, gender and ethnicity
- Contact details – your home address, home and mobile telephone numbers, email address
- Details of your previous qualifications
- Information about your nationality and residency to determine funding eligibility
- Information about medical/health conditions and learning disabilities or difficulties

We collect parent/carer details (name, address, email, telephone numbers) under GDPR Article 6d (Vital Interests) and Article 6e (Public Task) in order to support our duty to support the education and learning as fully as possible. Some data we will collect and process with your consent, such as surveys and photos for marketing.

We collect your gender and ethnicity under GDPR Article 9e for equal opportunity monitoring.

Collecting student information

Most of the information above is collected directly from yourself via an application or enrolment form. A medical form is completed by your parent/carer after you have been given an offer or have enrolled. Some information such as previous qualifications may

be collected or verified from other organisations such as the Learner Records Service or your previous school.

Failure to provide data required to meet legal obligations will result in us not being able to enrol you as a student. Failure to provide other information, for example learning difficulty information, may result in the college being unable to provide the standard of service we would wish to provide.

Storing your data

We hold your data securely on the College's databases and on paper in a locked environment. We retain applicant data for one year after the application process has finished so that we can effectively deal with re-applications. We retain student data for six years after you leave the College. We do this so that we can provide a reference for you if you need one or if you need to confirm you were a student here for other reasons. As such, we cannot act as a referee for you after six years after you have left the College.

Updating your data

We have a duty to keep your data up to date so will periodically ask you to check that it is all still correct. You can submit changes to your details via Woodle and you can request a new ID photograph via the attendance team.

Who we share student information with

We share aspects of your personal information with:

- staff currently employed at the College to provide services to our students
- your previous school to inform us of your needs and them of your destination after college
- the funding agency and the Department for Education to meet our legal obligations and receive funding (see their privacy notice <https://www.gov.uk/government/publications/esfa-privacy-notice>)
- exam awarding bodies to register you for exams and make Access Arrangements
- universities and employers who may ask us for a reference or CV
- your parents/carers to keep them informed of your progress
- Tucasi and the college caterers to provide a cashless catering system and free school meal allowances
- ALPS and the SFCA (Six Dimensions) to monitor retention and achievement
- educational-related services and tools to help you in your learning and experience at college such as Kerboodle, MyConcern, MyMaths, MEI, Unifrog, Google for Google Classroom and Microsoft for Office 365
- Sport England to support increased sport and physical activity in England
- Barnet Council to support the Raising the Participation Age initiative
- police, CAMHS, social services organisations, local councils and other agencies as the need arises
- hosts for trips and the organisation of visits

Where Woodhouse College uses proprietary software subscriptions to process personal data on its behalf, we require them to do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Why we share student information

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.

We share students' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

LRS Data Sharing Agreement:

The information you supply will be used by the Skills Funding Agency, an executive agency of the Department for Education (DfE), to issue you with a Unique Learner Number (ULN), and to create your Personal Learning Record. For more information about how your information is processed and shared refer to the Extended Privacy Notice available on Gov.UK

Requesting access to your personal data

Under data protection legislation, parents and students have the right to request access to information about them that we hold. To make a request for your personal information contact the College's Data Protection Officer (DPO).

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- have inaccurate personal data rectified, and, in certain circumstances, data can be blocked, erased or destroyed;
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>.

The Right to be Forgotten

Students, parents, staff, governors and other users of the College have the right to obtain the erasure of personal data where this data is no longer necessary in relation to the purposes for which they were collected and processed. However, there are certain limits on this right, such as the need to retain data for funding or safeguarding and obligations.

Any person who wishes to exercise this right should complete the college "Subject Access Request" form and submit it to the College Data Protection Officer. (Completion of this form is not mandatory but doing so will accelerate a request)

The College may charge a fee if the request is manifestly unfounded or excessive.

The College aims to comply with requests as quickly as possible, but will ensure that it is provided within one month unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the person making the request.

Contact

If you have any questions or would like to discuss anything in this privacy notice, please contact:

Beth Yap
Data Protection Officer
Woodhouse College
Woodhouse Road
Finchley
London N12 9EY

020 8445 1210

DPO@woodhouse.ac.uk

Privacy Notice for Staff

How we use college workforce information

Woodhouse College uses your personal information because it is or may become your employer. We use applicant information for our recruitment processes and some of the information you give us at this stage will become part of your personal data as an employee if you are appointed. On appointment, the College asks for proof of your qualifications and collects further details from you in relation to our responsibility for safeguarding young people, issuing your contract, paying your salary, and aspects of your welfare, health and safety. We monitor the work of our staff and how that develops over time so we record information about the roles you undertake for the College and how you perform in them through probationary and appraisal systems. We record the professional development you undertake, any formal communications you make with us and any absences from work. This information will form the basis of a reference should you ask us to provide one for you.

This notice gives you more information about how the College collects, stores, processes and shares your data.

The categories of college workforce information that we collect, process, hold and share include:

- personal information (such as your name, employee or teacher number, national insurance number, copies of documents which we use to confirm your identity and proof of address)
- special categories of data including information about your personal characteristics such as your gender, age, ethnic group
- your DBS (Disclosure Barring Services) disclosure number and date of clearance in our Single Central Record
- contract information (such as start dates, hours worked, post, roles and salary information)
- your bank details
- a photograph of you for your ID badge and staff gallery
- further photographs you let us use to communicate the work of the College and for marketing purposes
- work absence information (such as dates of absences and reasons, including annual leave)
- medical, health and occupational health information
- fitness for work notes and self-certification forms
- personal risk assessments, action plans and follow up notes
- maternity certificates
- your qualifications achieved prior to your employment if these are a requirement of the job, and those you tell us about subsequently
- the continuing personal development (CPD) you undertake during your employment
- visits you undertake as part of your employment

- dietary and medical requirements usually in relation to day visits and residential trips
- your driving licence details if you drive a College vehicle
- appraisal and performance management records
- documents regarding any disciplinary or capability proceedings
- detail concerning the roles you undertake and your timetable where relevant
- a record of any books and other resources you borrow from the College
- a record of expenses you claim
- a copy of any references about you and those we provide for you
- pension-related documents and records
- information you tell us about yourself during your employment such as any criminal convictions (that are not part of a DBS check)
- any other formal, written correspondence you make with the College as your employer or which we make with you
- some of what you write as part of the work you do such as emails or printed information

Why we collect and use this information

We use college workforce data to:

- inform staff recruitment decisions
- build and maintain an accurate picture of your work
- inform the development of recruitment and retention policies
- ensure you are paid, including deductions for pensions and taxes
- ensure the safeguarding of our students
- assess the College's effectiveness overall and the work of its various departments and faculties
- plan future developments and priorities as well as strategic and financial planning
- monitor and manage staff performance so that it reflects College priorities and targets
- be a responsible employer such as for staff health and safety
- plan and resource CPD
- publicise and explain the work of the College
- organise teaching and other functions
- track the deployment of resources such as funds, books and IT equipment
- respond appropriately when there are disciplinary and capability issues
- enable you to apply for and progress on to other roles and opportunities

The lawful basis on which we process this information

We process this information which is deemed personal data and special categories of data under GDPR 2018, Article 6, for at least one of the following reasons:

- a) **Consent:** you have given clear consent for us to process your personal data for a specific purpose.
- b) **Contract:** the processing is necessary for a contract we have with you

- c) **Legal obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).
- d) **Vital interests:** the processing is necessary to protect someone's life.
- e) **Public task:** the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
- f) **Legitimate interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect your personal data which overrides those legitimate interests.

We collect sensitive personal data under GDPR Article 9e for equal opportunity monitoring.

Storing this information

We hold your data securely on the College's databases and on paper in a locked environment. We retain staff applicant data for six months after the application process has finished so that we can effectively deal with re-applications. We hold college workforce data for the duration of your employment at the College and for six years following the year you leave the College's employment. In the event of a civil courts claim, records can be requested dating back six years after you have left employment under the Limitation Act 1980.

Who we share this information with

We may share your information with:

- Software for People – payroll provider
- Teachers' Pension Service
- Local Government Pension Service – support staff pension provider
- Strictly Education – DBS registered body
- Alps and the SFCA (Six Dimensions) for student progress analysis
- Kiddivouchers – childcare voucher provider
- Tucasi and the College caterers
- Educational-related services and tools such as MyMaths, MEI, Unifrog, Google for Google Classroom and Microsoft for Office 365

We may disclose personal information to the police or the Department for Education Teaching Regulation Agency in relation to investigations which involve staff members.

Where Woodhouse College uses proprietary software subscriptions to process personal data on its behalf, we require them to do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Why we share college workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so. The main reasons we share workforce data are:

- for salaries and other reimbursements to be paid
- for pension contributions and other salary deductions to be made
- for safeguarding reasons and to enter and exit the site
- to organise and assess the work of the College using proprietary IT systems and to enable staff to retrieve relevant information from those systems
- to enable staff to borrow resources such as those in the Library
- to enable staff to make payments when they need to such as to use the canteen
- to enable staff to access systems and facilities which help them with their work

Requesting access to your personal data

Under data protection legislation, you have the right to make a formal request to access information that we hold about you. To make an access request for your personal information, contact Beth Yap, Data Protection Officer.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- have inaccurate personal data rectified, and, in certain circumstances, data can be blocked, erased or destroyed;
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>.

The Right to be Forgotten

Students, parents, staff, governors and other users of the College have the right to obtain the erasure of personal data where this data is no longer necessary in relation to the purposes for which they were collected and processed. However, there are certain limits on this right, such as the need to retain data for funding or safeguarding and obligations.

Any person who wishes to exercise this right should complete the college "Subject Access Request" form (and submit it to the College Data Protection Officer. (Completion of this form is not mandatory but doing so will accelerate a request)

The College may charge a fee if the request is manifestly unfounded or excessive. The College aims to comply with requests as quickly as possible, but will ensure that it is provided within one month unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the person making the request.

Contact

If you have any questions or would like to discuss anything in this privacy notice, please contact:

Beth Yap
Data Protection Officer
Woodhouse College
Woodhouse Road
Finchley
London N12 9EY

020 8445 1210

DPO@woodhouse.ac.uk

Privacy Notice for Governors

How we use governor information

Woodhouse College uses your personal information to fulfil its obligation to maintain the Corporation as its senior decision-making body. We use this information to contact you regarding Board business, provide returns required by funding agencies and government departments and for inclusion in Board minutes and reports. This notice gives you more information about how the College collects, stores, processes and shares your data.

The categories of information that we collect, process, hold and share include:

- personal information (such as your name, email address and copies of documents which we use to confirm your identity and proof of address)
- business or pecuniary interests that you may hold
- special categories of data including information about your personal characteristics such as your gender, age, ethnic group
- your DBS (Disclosure Barring Services) disclosure number and date of clearance in our Single Central Record
- a photograph of you for your ID badge
- your continuing personal development
- a log of your skills and sector experience
- information you tell us about yourself, such as any criminal convictions (that are not part of a DBS check)

Why we collect and use this information

We use this data to:

- inform governor recruitment decisions
- for inclusion in Board and Committee minutes
- for inclusion in the annual report and financial statements
- to maintain register of interests containing declarations from each governor
- to ensure that governors have not been disqualified as a charity trustee in accordance with the Charities Act 2006
- to maintain a skills audit
- ensure the safeguarding of our students
- assess the College's effectiveness overall.

The lawful basis on which we process this information

We process this information which is deemed personal data and special categories of data under GDPR 2018, Article 6, for at least one of the following reasons:

- a) **Consent:** you have given clear consent for us to process your personal data for a specific purpose.
- b) **Contract:** the processing is necessary for a contract we have with you
- c) **Legal obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).
- d) **Vital interests:** the processing is necessary to protect someone's life.
- e) **Public task:** the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
- f) **Legitimate interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect your personal data which overrides those legitimate interests.

We collect sensitive personal data under GDPR Article 9e for equal opportunity monitoring.

Storing this information

We hold your data securely on the College's databases and on paper in a locked environment. We retain applicant data for six months after the application process has finished so that we can effectively deal with re-applications. We hold your data for the duration of your term of office at the College and for six years after you leave the College.

Who we share this information with

We may share your information with:

- Strictly Education – DBS registered body
- Trust Governor
- Department for Education
- Staff and other governors

We may disclose personal information to the police or the Department for Education in relation to investigations, which involve governors.

Where Woodhouse College uses proprietary software subscriptions to process personal data on its behalf, we require them to do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Why we share information

We do not share information with anyone without consent unless the law and our policies allow us to do so. The main reasons we share data are:

- For governors to be able to access papers via the online portal, Trust Governor
- To be able to carry out a DBS check

Requesting access to your personal data

Under data protection legislation, you have the right to make a formal request to access information that we hold about you. To make an access request for your personal information, contact Beth Yap, Data Protection Officer.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- have inaccurate personal data rectified, and, in certain circumstances, data can be blocked, erased or destroyed;
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>.

The Right to be Forgotten

Students, parents, staff, governors and other users of the College have the right to obtain the erasure of personal data where this data is no longer necessary in relation to the purposes for which they were collected and processed. However, there are certain limits on this right, such as the need to retain data for funding or safeguarding and obligations.

Any person who wishes to exercise this right should complete the college "Subject Access Request" form and submit it to the College Data Protection Officer. (Completion of this form is not mandatory but doing so will accelerate a request)

The College may charge a fee if the request is manifestly unfounded or excessive. The College aims to comply with requests as quickly as possible, but will ensure that it is provided within one month unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the person making the request.

Contact

If you have any questions or would like to discuss anything in this privacy notice, please contact:

Beth Yap
Data Protection Officer
Woodhouse College
Woodhouse Road
Finchley
London N12 9EY

020 8445 1210

DPO@woodhouse.ac.uk



Privacy Notice for Former Students Entering Exams

How we use your information

Woodhouse College uses your personal information in order to provide you with exam-related services. This is necessary so that it is clear what exams you are taking, to provide you with a timetable, to contact you when we need to, to enter you for the right exams, to carry out our safeguarding duties and inform you of your exam outcomes and certification. All of these activities require that we hold your personal data and this notice gives you more information about how and why we do this.

The categories of information that we collect, hold and share to process your application to sit exams and to administer, schedule and run those exams:

- Personal information (such as your name, and address), contact information.
- Your exam entries and your results in exams taken at College

Why we collect and use this information

We use your data when you have applied to take exams:

- to identify you and keep the College safe
- to enter you for exams
- to give you an exam timetable
- to request exam access arrangements or support during exams if necessary
- to enable you to make online payments
- to apply for special consideration if required
- to issue results and certificates to you

The lawful basis on which we process this information

We process this information which is deemed personal data and special categories of data under GDPR 2018, Article 6, for at least one of the following reasons:

- a) **Consent:** you have given clear consent for us to process your personal data for a specific purpose.
- b) **Contract:** the processing is necessary for a contract we have with you
- c) **Legal obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).
- d) **Vital interests:** the processing is necessary to protect someone's life.
- e) **Public task:** the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

- f) **Legitimate interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect your personal data which overrides those legitimate interests.

Collecting your information

The information above is collected directly from yourself via an exam entry application form.

Storing this information

We hold your data securely on the College's databases and on paper in a locked environment. We retain this information for six years following the year in which your exam results are issued.

Who we share this information with

We share aspects of your personal information with:

- staff currently employed at the College to provide services to you
- exam awarding bodies to register you for exams and make Access Arrangements
- universities and employers who may ask us for a reference or CV

Where Woodhouse College uses proprietary software subscriptions to process personal data on its behalf, we require them to do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Why we share student information

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.

We share students' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

Requesting access to your personal data

Under data protection legislation, you have the right to make a formal request to access information that we hold about you. To make an access request for your personal information, contact Beth Yap, Data Protection Officer.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress

- prevent processing for the purpose of direct marketing
- have inaccurate personal data rectified, and, in certain circumstances, data can be blocked, erased or destroyed;
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>.

The Right to be Forgotten

Students, parents, staff, governors and other users of the College have the right to obtain the erasure of personal data where this data is no longer necessary in relation to the purposes for which they were collected and processed. However, there are certain limits on this right, such as the need to retain data for funding or safeguarding and obligations.

Any person who wishes to exercise this right should complete the college "Subject Access Request" form and submit it to the College Data Protection Officer. (Completion of this form is not mandatory but doing so will accelerate a request.)

The College may charge a fee if the request is manifestly unfounded or excessive. The College aims to comply with requests as quickly as possible, but will ensure that it is provided within one month unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the person making the request.

Contact

If you have any questions or would like to discuss anything in this privacy notice, please contact:

Beth Yap
Data Protection Officer
Woodhouse College
Woodhouse Road
Finchley
London N12 9EY
020 8445 1210
DPO@woodhouse.ac.uk

Subject Access Request

Recital 63 of the General Data Protection Regulations (GDPR) states *a data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing.* Data subjects are also able to request the erasure of their data if it is no longer necessary in relation to the purposes for which it was collected and processed. However, there are certain limits on this right, such as the need to retain data for funding or safeguarding and obligations.

You can request to access your data via phone, email or verbally. However in order to process your request as quickly and efficiently as possible we would ask that you complete this form. You will also need to provide proof of identity, usually this would be by communicating via an email address that the College already has on file for you. However if this cannot be done, proof of identity (such as a birth certificate, passport, driving licence or an official letter addressed to you at your home address) would need to be provided. Your request will be processed within 30 calendar days on receipt of a completed form and proof of identity.

Woodhouse College does not charge for subject access requests. However, the College may charge a fee if the request is manifestly unfounded or excessive.

Please provide the below information and return this form to:

Beth Yap (Data Protection Officer) DPO@woodhouse.ac.uk
Woodhouse College,
Woodhouse Road,
Finchley, London,
N12 9EY

Personal Information

Title:

Surname:

First Name(s):

Date of Birth:

Address:

Previous Address (Known to the College):

Telephone number:

Please outline below the details of your request.

Are you requesting the erasure of your data?

Yes

No

Please tick the box below that is relevant to the data held by the College:

Employment Information

Student Information

Please provide the dates you attended/were employed by the College. Please also provide your learner/employee number if possible.

Declaration:

I confirm that the information provided on this form is correct to the best of my knowledge and that I am the person to whom it relates. I understand that Woodhouse College is obliged to confirm proof of identity and it may be necessary to obtain further information in order to comply with this subject access request.

Name

Signature

Date

Data Breach Notification Procedure

Woodhouse College holds, processes and shares a large amount of personal data. Every care is taken to protect personal data and avoid a data protection breach that could compromise security.

The Scope of this Procedure

This procedure relates to all personal and sensitive data held by the College, regardless of format. The procedure applies to all staff and students at the College, including contractors, consultants, suppliers and data processors working for, or on behalf of the College.

The objective of this procedure is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

Types of Breach

For the purpose of this procedure, data security breaches include both confirmed and suspected incidents. An incident, in the context of this procedure, is an event or action, which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately.

An incident includes, but is not restricted to:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (for example loss of a laptop, tablet device, mobile phone or paper record).
- Unauthorised use of, access to or modification of data or information systems.
- Attempts to gain unauthorised access to information or IT systems, regardless of whether these attempts were failed or successful.
- Unauthorised disclosure of sensitive or confidential data.
- Unforeseen circumstances such as a fire or flood.
- Other human error.

Responding to Personal Data Breaches

All staff at Woodhouse College must report any actual or possible data breach immediately (within 12 hours of becoming aware of the breach) to the Data Protection Officer by emailing DPO@woodhouse.ac.uk

The report will include full and accurate details of the incident, when the breach occurred, who is reporting it, the nature of the information and how many individuals were involved.

Containment and Recovery

The Data Protection Officer will determine if the breach is still occurring and, if so, the appropriate steps will be taken to immediately minimise the effect of the breach.

The steps taken by the Data Protection Officer when responding to a personal data breach may include:

- Ensuring that the personal data breach is contained as soon as possible.
- Assessing the level of risk to data subjects as soon as possible.

- Gathering and collating information from relevant sources.
- Informing all interested persons within the College of the personal data breach and the investigation.
- Assessing the level of risk to the College.
- Notifying supervisory authorities (with 72 hours), data controllers, data subjects and others of the breach in accordance with this procedure.

The Data Protection Officer is primarily responsible for investigating possible or actual personal data breaches and for determining whether any notification obligations apply. The investigation will need to take into account the following:

- The type of data involved and its sensitivity
- The protections that are in place
- What has happened to the data (for example if it has been lost or stolen)
- Whether the data could be put to any illegal or inappropriate use
- Who the individuals are, the number of individuals involved and the potential effect on those data subjects.
- Whether there are wider consequences to the breach.

All staff must cooperate with the Data Protection Officer in relation to the investigation and notification of personal data breaches.

Notification

The Data Protection Officer is responsible for determining who needs to be notified of the breach and every incident will be assessed on a case-by-case basis.

Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Information on what action has already been taken to mitigate risks should also be shared along with advice on what the individuals can do to protect themselves further. Individuals should also be provided with a way to contact the College if they have any further concerns or questions about the breach.

If a large number of people are affected or there are serious consequences the Information Commissioner's Office (ICO) should be notified.

The Data Protection Officer will keep a full record of the breach, including the details of the breach, its effects and the remedial action taken.

Evaluation

Once the initial incident is contained the Data Protection Officer will carry out a full review of the causes of the breach; the effectiveness of the responses and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy and whether any further action is needed to minimise the risk of similar incidents occurring.

The review will consider:

- Where and how personal data is held and stored.
- Where the biggest risks lie and whether there are any concerns regarding existing measures.
- Staff awareness.