Weston College

Data Protection Policy and Privacy Notices

Written by	Peter Sloman	
Reviewed by	Weston College	
Approved by	Weston College Corporation	
Date of Review:	01/05/2019	
Next Review:	01/05/2020	

Signed: ……

Date: ……

Contents

1. Aims

Weston College aims to ensure that all personal data collected about staff, learners, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreements and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

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

4. The data controller

Weston College processes personal data relating to parents, learners, staff, governors, visitors and others, and therefore is a data controller.

Weston College is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by Weston College, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The local governing board has overall responsibility for ensuring that Weston College complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on Weston College's data protection issues.

The DPO is also the first point of contact for individuals whose data Weston College processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Weston College's DPO is Peter Sloman and is contactable via DataProtectionOfficer@weston.ac.uk

5.3 Principal and Chief Executive

Weston College's Principal and Chief Executive acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing Weston College of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that Weston College must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how Weston College aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

Weston College will only process personal data where Weston College have at least one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that Weston College can **fulfil a contract** with the individual, or the individual has asked Weston College to take specific steps before entering into a contract
- The data needs to be processed so that Weston College can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that Weston College, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of Weston College or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a learner) has freely given clear **consent**

For special categories of personal data, Weston College will also meet one of the special category conditions for processing which are set out in the GDPR Article 9 and Data Protection Act 2018.

Whenever Weston College first collect personal data directly from individuals, Weston College will provide them with the relevant information required by data protection law on how their data is processed

7.2 Limitation, minimisation and accuracy

Weston College will only collect personal data for specified, explicit and legitimate reasons. Weston College will explain these reasons to the individuals when Weston College first collect their data.

If Weston College want to use personal data for reasons other than those given when Weston College first obtained it, Weston College will inform the individuals concerned before Weston College do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done as set out in Weston College's Privacy Policy available on Weston College's website.

8. Sharing personal data

Weston College will not normally share personal data with anyone else, but may do so where:

- There is an issue with a learner or parent/carer that puts the safety of our staff or other students at risk
- Weston College need to liaise with other agencies – Weston College will seek consent if Weston College cannot rely on any other lawful bases before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and learners – for example, IT companies. When doing this, Weston College will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data Weston College share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

Weston College will also share personal data with law enforcement and government bodies where Weston College are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

Weston College may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our learners or staff.

Where Weston College transfer personal data to a country or territory outside the European Economic Area, Weston College will do so in accordance with data protection law.

Any final decision in data sharing will be referred to the Principal and Chief Executive who may also liaise with the Chair of Governors of the Corporation.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that Weston College holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of learners at Weston College may not be granted without the express permission of the learner. This is not a rule and a learner's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, Weston College:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual Weston College will comply within 3 months of receipt of the request, where a request is complex or numerous. Weston College will inform the individual of this within 1 month, and explain why the extension is necessary

Weston College will not disclose information if it:

- Might cause serious harm to the physical or mental health of a learner or another individual
- Would reveal that a child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child
- Is going to cause serious harm to the physical or mental health of Staff

If the request is unfounded or excessive, Weston College may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When Weston College refuse a request, Weston College will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when Weston College are collecting their data about how Weston College use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to the processing of data, where consent is needed to process it, at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest

- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a learner) within 15 working days of receipt of a written request.

11. CCTV

Weston College use CCTV in various locations around all Weston College sites to ensure it remains safe. Weston College will adhere to the ICO's code of practice for the use of CCTV.

Weston College do not need to ask individuals' permission to use CCTV, but Weston College make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the DPO.

12. Photographs and videos

As part of Weston College activities, Weston College may take photographs and record images of individuals within Weston College.

Weston College will obtain written consent, for photographs and videos to be taken of learners and staff? for communication, marketing and promotional materials.

Uses may include:

- Within Weston College on notice boards and in Weston College magazines, brochures,
- Outside of Weston College by external agencies such as Weston College photographer, newspapers, campaigns
- Online on Weston College website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, Weston College will delete the photograph or video and not distribute it further.

When using photographs and videos in this way Weston College will not accompany them with any other personal information about the learner, to ensure they cannot be identified unless this has been explicitly agreed beforehand, for example on posters describing a learners journey and progression route.

For more information on our use of photographs and videos please contact the DPO.

13. Data protection by design and default

Weston College will put measures in place to show that Weston College have integrated data protection into all data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where Weston College's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; Weston College will also keep a record of attendance
- Regularly conducting reviews and audits to test privacy measures and make sure Weston College are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of Weston College and DPO and all information Weston College are required to share about how Weston College use and process personal data (via privacy notices)
    - For all personal data that Weston College hold, maintaining an internal record of the type of data, data subject, how and why Weston College are using the data, any third-party recipients, how and why Weston College are storing the data, retention periods and how Weston College are keeping the data secure

14. Data security and storage of records

Weston College will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from their associated Weston College office
- Passwords that are at least 8 characters long containing letters and numbers are used to access Weston College computers, laptops and other electronic devices. Staff and learners are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, learners or governors who store personal information on their personal devices are expected to follow the same security procedures as for Weston College-owned equipment
- Where Weston College need to share personal data with a third party, Weston College carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where Weston College cannot or do not need to rectify or update it.

For example, Weston College will shred or incinerate paper-based records, and overwrite or delete electronic files. Weston College may also use a third party to safely dispose of records on Weston College's behalf. If Weston College do so, Weston College will require the third party to provide sufficient guarantees that it complies with data protection law.

See Weston College's Document Retention Policy for further detailed information on the disposal of records and personal data.

16. Personal data breaches

Weston College will make all reasonable endeavors to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, Weston College will follow the procedure set out in appendix 1.

When appropriate, Weston College will report the data breach to the ICO within 72 hours. Such breaches in a Weston College context may include, but are not limited to:

- A non-anonymised dataset being published on the Weston College website which shows the exam results of learners eligible for pupil premium, bursary and free school meals
- Safeguarding information being made available to an unauthorised person
- The theft of a Weston College laptop containing non-encrypted personal data about learners

17. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or Weston College's processes make it necessary.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect Weston College's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Confidential Waste Procedure
- Data Retention Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the Principal and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on Weston College's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on Weston College's computer system.
- The DPO and Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

Weston College will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. Weston College will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email or any other method (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO make all reasonable endeavours to ensure Weston College receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, Weston College will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

Appendix 2: Privacy notice – Use of workforce recruitment information

Privacy Notice (How we use workforce recruitment information)

Under data protection law, individuals have a right to be informed about how Weston College uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use your personal data and data about you.

We, Weston College are the 'data controller' for the purposes of data protection law.

Our data protection officer is Peter Sloman

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

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration, including benefit entitlements;
- whether or not you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process;
- information about your entitlement to work in the UK; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health, and religion or belief.

Why we collect and use this information

The College needs to process data to take steps at your request prior to entering into a contract with you. It also needs to process your data to enter into a contract with you.

In some cases, the College needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

The College has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the College to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. The College may also need to process data from job applicants to respond to and defend against legal claims.

Where the College relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

The College processes health information if it needs to make reasonable adjustments to the recruitment process for candidates who have a disability. This is to carry out its obligations and exercise specific rights in relation to employment.

Where the College processes other special categories of data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is for equal opportunities monitoring purposes.

The College will not use your data for any purpose other than the recruitment exercise for which you have applied.

The lawful basis on which we process workforce information under Article 6 of GDPR is as follows:

"(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;"

and/or

"(c) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;"

Where data processed is classified as special category data under GDPR, the lawful basis on which we process workforce information under Article 9 of GDPR is as follows:

"(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;"

We only collect and use workforce personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process workforce recruitment personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use workforce recruitment personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using workforce recruitment personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

The College collects this information in a variety of ways. For example, data might be contained in application forms, CVs, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment.

The College will also collect personal data about you from third parties, such as references supplied by former employers and information from disclosure and barring checks. The College will only seek information from the DBS once a job offer to you has been made and will inform you that it is doing so. References will only be obtained in advance of an offer being made if you have specified that we can contact your referees prior to interview.

You are under no statutory or contractual obligation to provide data to the organisation during the recruitment process. However, if you do not provide the information, the organisation may not be able to process your application properly or at all.

You are under no obligation to provide information for equal opportunities monitoring purposes and there are no consequences for your application if you choose not to provide such information.

Storing this information

Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).We may also keep it beyond their employment if this is necessary in order to comply with our legal obligations.

When data is stored and/or retained, we will continually:

- review the length of time we keep personal data;
- consider the purpose or purposes that we hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes;
- update, archive or securely delete information if it goes out of date or is no longer required

If your application for employment is unsuccessful, the organisation will hold your data on file for 1 year after the end of the relevant recruitment process. At the end of that period (or once you withdraw your consent), your data is deleted or destroyed.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file (and retained during your employment). The periods for which your data will be held will be provided to you in a new privacy notice.

The College takes the security of your data seriously. It has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties.

Who we share this information with

Your information will be shared internally for the purposes of the recruitment exercise. This includes members of the HR team, interviewers involved in the recruitment process and managers in the business area with the vacancy.

We will only share your information with partners or suppliers who have sufficient measures and procedures in place to protect your information and can meet their legal obligations under data protection legislation.

We routinely share anonymised information with:

- Our local authority
- Office for National Statistics
- Internal and external auditors
- Awarding organisations
- Other external organisations in the pursuit of business interests.

With the exception of the above the College will not share your data with third parties, unless you have specified that we can or if your application for employment is successful and it makes you an offer of employment.

Why we share 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.

Data collection requirements

JOB APPLICANTS, CURRENT EMPLOYEES AND FORMER EMPLOYEES

How we use your information

The information we ask for is used to assess your suitability for employment. You don't have to provide what we ask for but it might affect your application if you don't.

Application stage

We ask you for your personal details including name and contact details. We will also ask you about your previous experience, education, referees and for answers to questions relevant to the role you have applied for.

Our recruitment team will have access to all of this information.

You will also be asked to provide equal opportunities information. This is not mandatory information – if you don't provide it, it will not affect your application. This information will not be made available to any staff outside of our recruitment team, including hiring managers, in a way which can identify you. Any information you do provide will be used only to produce and monitor equal opportunities statistics.

Shortlisting

Our hiring managers shortlist applications for interview. They will not be provided with your contact details or with your equal opportunities information if you have provided it.

Candidates are asked to provide proof of identity and qualifications at the interview. Photocopies of original documents are only retained if the candidate is successful.

If you are unsuccessful for the position you have applied for, your data will be held for a period of 1 year in case of any queries regarding the outcome, for feedback purposes or for recruitment analysis.

Conditional offer

If we make a conditional offer of employment, we will ask you for information so that we can carry out pre-employment checks. You must successfully complete pre-employment checks to progress to a final offer. We are required to confirm the identity of our staff, their right to work in the United Kingdom and assess suitability for the role.

Upon your acceptance of a final offer your data will be transferred to your personnel file (and retained during your employment). The periods for which your data will be held will then be subject to the privacy policy: How we use workforce information.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact Caroline Pringle, HR Manager, Weston College or Peter Sloman, Data Protection Officer, Weston College.

You also have the right to:

- access and obtain a copy of your data on request
- require the organisation to change incorrect or incomplete data
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing
- object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing
- ask the College to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the College's legitimate grounds for processing data
- 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 ask 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/

Further information

If you would like to discuss anything in this privacy notice, please contact:

Peter Sloman, Data Protection Officer, Weston College

Appendix 3: Privacy notice – Use of workforce information

Privacy Notice (How we use workforce information)

Under data protection law, individuals have a right to be informed about how Weston College uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use your personal data and data about you.

We, Weston College are the 'data controller' for the purposes of data protection law.

Our data protection officer is Peter Sloman

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

- your name, address and contact details, including email address and telephone number, date of birth and gender
- the terms and conditions of your employment
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover
- details of your bank account and national insurance number
- information about your marital status, next of kin, dependants and emergency contacts
- information about your nationality and entitlement to work in the UK
- information about your criminal record
- details of your schedule (days of work and working hours) and attendance at work
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments
- details of trade union membership
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief

Why we collect and use this information

The College needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements.

In some cases, the College needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. For all positions, it is necessary to carry out criminal records checks to ensure that individuals are permitted to work within the College.

In other cases, the College has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the College to:

- run recruitment and promotion processes

- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled
- ensure effective general HR and business administration, this includes using the data to help test the HR system as appropriate
- provide references on request for current or former employees
- respond to and defend against legal claims
- maintain and promote equality in the workplace

Where the College relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes).

Where the College processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that the organisation uses for these purposes is anonymised or is collected with the express consent of employees, which can be withdrawn at any time. Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

The lawful basis on which we process this information

You have some obligations under your employment contract to provide the College with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the College with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the College to enter a contract of employment with you. If you do not provide other information, this will hinder the College's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

The lawful basis on which we process workforce information under Article 6 of GDPR is as follows:

“(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;”

and/or

“(c) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;”

Where data processed is classified as special category data under GDPR, the lawful basis on which we process workforce information under Article 9 of GDPR is as follows:

"(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;"

We only collect and use workforce personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process workforce personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use workforce personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using workforce personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

The College collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the College collects personal data about you from third parties, such as references supplied by former employers, and information from criminal records checks permitted by law.

Data is stored in a range of different places, including in your personnel file, in the College's HR management systems and in other IT systems (including the College's email system).

Storing this information

The College takes the security of your data seriously. The College has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where the College engages third parties to process personal data on its behalf, they 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.

The College will hold your personal data for the duration of your employment. Your data is held for 7 years after the end of your employment. At the end of that period (or once you withdraw your consent), your data is deleted or destroyed.

When data is stored and/or retained, we will continually:

- review the length of time we keep personal data;
- consider the purpose or purposes that we hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes;
- update, archive or securely delete information if it goes out of date or is no longer required

Who we share this information with

Your information will be shared internally, including with members of the HR team, the finance department, your line manager, managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles.

The College shares your data with third parties in order to obtain references from other employers and obtain necessary criminal records checks from the Disclosure and Barring Service. The College may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The College also shares your data with third parties that process data on its behalf, in connection with payroll, pension scheme providers, the provision of benefits and the provision of occupational health services.

We will only share your information with partners or suppliers who have sufficient measures and procedures in place to protect your information and can meet their legal obligations under data protection legislation.

Why we share 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.

Data collection requirements

JOB APPLICANTS, CURRENT EMPLOYEES AND FORMER EMPLOYEES

How we use your information

The information we ask for is used to assess your suitability for employment. You don't have to provide what we ask for but it might affect your application if you don't.

Application stage

We ask you for your personal details including name and contact details. We will also ask you about your previous experience, education, referees and for answers to questions relevant to the role you have applied for.

Our recruitment team will have access to all of this information.

You will also be asked to provide equal opportunities information. This is not mandatory information – if you don't provide it, it will not affect your application. This information will not be made available to any staff outside of our recruitment team, including hiring managers, in a way which can identify you. Any information you do provide will be used only to produce and monitor equal opportunities statistics.

Shortlisting

Our hiring manager's shortlist applications for interview. They will not be provided with your name or contact details or with your equal opportunities information if you have provided it.

Candidates are asked to provide proof of identity and qualifications at the interview. Photocopies of original documents are only retained if the candidate is successful.

If you are unsuccessful for the position you have applied for, your data will be held for a period of six months in case of any queries regarding the outcome or for feedback purposes.

Conditional offer

If we make a conditional offer of employment, we will ask you for information so that we can carry out pre-employment checks. You must successfully complete pre-employment checks to progress to a final offer. We are required to confirm the identity of our staff, their right to work in the United Kingdom and assess suitability for the role.

Upon commencement of your employment, we will also ask you for:

Bank details – to process salary payments

Emergency contact details – so we know who to contact in case you have an emergency at work

Employment status for tax code purposes.

Our contract of employment requires all staff to declare if they have any potential conflicts of interest, other employment or engagement. If you complete a declaration, the information will be held on your personnel file.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact Caroline Pringle, HR Manager, Weston College or Peter Sloman, Data Protection Officer, Weston College.

You also have the right to:

- access and obtain a copy of your data on request;
- require the College to change incorrect or incomplete data;
- require the College to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where the College is relying on its legitimate interests as the legal ground for processing; and
- ask the College to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the College's legitimate grounds for processing data or 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 ask 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/

Further information

If you would like to discuss anything in this privacy notice, please contact:

Peter Sloman, Data Protection Officer, Weston College

Appendix 4: Privacy notice – Use of learners', parents' and guardians' personal data

Privacy Notice (Use of learners', parents' and guardians' personal data)

Under data protection law, individuals have a right to be informed about how Weston College uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use your personal data and data about your child/learners.

We, Weston College are the 'data controller' for the purposes of data protection law.

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

Personal data that we may collect, use, store and share (when appropriate) about learners and/or parents/guardian includes, but is not restricted to:

- personal information (such as name, unique learner number and address);
- characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility);
- photographs including the use of photographs on social media;
- attendance information (such as sessions attended, number of absences and absence reasons);
- information about special educational needs and disabilities (SEND) including whether a learner is the subject of a statement of SEND or holds an Educational Health Care Plan (EHCP);
- information about pupil premium funding, Free School Meals or bursary funding
- information about safeguarding including child in need, child protection categorisation;
- medical support needs;
- details of exclusions and behavioural information;
- post 16 learning information
- results of internal assessments and externally set tests
- learner and curricular records
- CCTV images captured on college premises

We may also hold data about learners that we have received from other organisations, including schools, local authorities and the Department for Education.

Why we collect and use this information

We use learner and parental/guardian data:

- to support learner learning
- to protect learner welfare
- to monitor and report on learner progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to contact parents/guardian when necessary

The lawful basis on which we process this information

The lawful basis on which we process learner information under Article 6 of GDPR is as follows:

"(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;"

and/or

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

and/or

"(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;"

Where data processed is classified as special category data under GDPR, the lawful basis on which we process learner information under Article 9 of GDPR is as follows:

"(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;"

We only collect and use learners' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process learners' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use learners' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using learners' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

While the majority of information we collect about learners is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

Storing this information

We keep personal information about learners while they are attending Weston College. We may also keep it beyond their attendance if this is necessary in order to comply with our legal obligations.

Learner data, as a standard, will be held for a period of six years from the end of the academic year in which you studied. Any variation that is required under our funding contract will be detailed in our Document Retention Strategy.

For all data we hold, we will continually:

- review the length of time (where not specified by law) we keep personal data
- consider the purpose or purposes that we hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes;
- update, archive or securely delete information if it goes out of date or is no longer required

Who we share learner information with

We do not share information about learners with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about learners and/or parents/guardians with:

- Our local authority
- Education and Skills Funding Agency
- The Department for Education (DfE)
- Office for Students (HE)
- National Offender Management Services (prison-based learners)
- National Apprenticeship Services
- Internal and external auditors
- Awarding organisations

Why we share learner information

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

Data collection requirements:

We share learners' data with the aforementioned organisations on a statutory basis. This data sharing underpins our further and higher education funding, educational attainment policy and monitoring and financial assurance processes.

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

The Individualised Learner Record (ILR)

The ILR is owned and managed by the Department for Education and contains information about learners in further and higher education colleges in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our learners to the DfE as part of statutory data collections such as the monthly ILR returns. The law that allows this is the Education (Information About Individual Learners) (England) Regulations 2013.

The department may share information about our Learners from the ILR with third parties who promote the education or well-being of young people and adults in England by:

- Conducting research or analysis
- Producing statistics
- Providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- Who is requesting the data
- The purpose for which it is required
- The level and sensitivity of data requested, and
- The arrangements in place to store and handle the data.

To be granted access to learner information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided learner information, (and for which project), please visit https://www.gov.uk/government/publications/national-Learner-database-requests-received

For DfE contact details, visit: https://www.gov.uk/contact-dfe

Learners aged 16+

We will also share certain information about learners aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority website.

Requesting access to your personal data

Under data protection legislation, learners have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Peter Sloman, Data Protection Officer, Weston College.

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
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- 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/

Further information

If you would like to discuss anything in this privacy notice, please contact **Peter Sloman, Data Protection Officer, Weston College.**