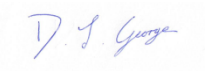
Weston College Group

Data Protection Policy

Data Protection Policy

CONTENTS

Change Control

Version:	1.1
Date approved by CLB:	01/09/2021 – via delegated authority  Darran George – Vice Principal
Date approved by Corporation:	N/a
Name of policy holder:	Matt Beaver – Head of IT
Date issued:	September 2021 (this version)
Review date:	August 2022

Version	Type – New/Replacement/Review	Date	History
1.0	New	December 2020	New policy
1.1	New/Replacement	September 2021	New policy that replaces the v1.0 Privacy Notice as recommended through data privacy review

Data Protection Policy

1 PURPOSE

1.1 Weston College Group is committed to ensuring that all personal data collected is processed under all relevant data protection laws including the UK General Data Protection Regulation (UK-GDPR) and the Data Protection Act 2018 (DPA 2018).

1.2 Weston College is registered as a data controller with the Information Commissioners Office (ICO). The certificate of registration is available from www.weston.ac.uk/dataprivacy

2 SCOPE

2.1 This policy applies to anyone who has access to and/or is a user of Weston College Group services premises or systems, including staff, governors, learners, volunteers, parents/carers, visitors, contractors, and other community users.

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

2.3 This policy is publicly available from www.weston.ac.uk/dataprivacy.

3 RESPONSIBILITIES

3.1 **Governing Body** - The Governing Body has overall responsibility for ensuring that Weston College Group complies with all relevant data protection obligations.

3.2 **Corporate Leadership Board (CLB)** - The Principal and the Chief Operating Officer acts with the delegated authority of the Governing Body on a day to day basis and will liaise with the DPO. In their absence, in case of emergency, any member of the Corporate Leadership Board (CLB) may be delegated this role.

3.3 **All staff** - All staff are responsible for:

- Familiarising themselves with and complying with this policy and acceptable use policies for staff. The learning culture within the organisation seeks the avoidance of blame culture and is key to allowing individuals the confidence to report genuine mistakes. However, staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken;
- Taking care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse at all times. All staff should adopt the approach that they should treat the personal data of others with the same care with which they would treat their own;
- Complying with IT & Data Security policies including:
    - Only using computers and other devices authorised by Weston College Group for accessing and processing personal data ensuring that they are properly “logged-off” at the end of any session in which they are using personal data;
    - Storing, transporting and transferring data using encryption
    - Using any personal devices following the Bring Your Own Device (BYOD) section of the IT Acceptable Use Policy.
- Deleting data in line with this policy and the retention schedule;
- Informing Weston College Group of any changes to their personal data, such as a change of address;
- Reporting to the Data Protection Officer (DPO) in the following circumstances:

- Any questions about the operation of this policy, data protection law, retaining or sharing personal data or keeping personal data secure;
- If they have any concerns that this policy is not being followed;
- If they are unsure whether they have a lawful basis upon which to use personal data in a particular way;
- If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the UK and European Economic Area;
- The discovery of a data breach or near miss (immediate action is required) – please refer to the Data Breach Policy section of this policy;
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
- If they are to share personal data with a data processor, for example, a contractor or someone offering a service, in which case a contract is likely to be required and potentially a data protection impact assessment

4 DATA PROTECTION OFFICER (DPO)

4.1 The Data Protection Officer (DPO) is responsible for advising on the implementation of this policy, monitoring compliance with data protection law, providing support and developing related policies and guidelines where applicable, amongst other data protection related functions. They get the Corporate Leadership Board (CLB) & The College Governing Body appraised on compliance and, where relevant, provide advice and recommendations on data protection issues.

4.2 Weston College Group has appointed a Data Protection Officer who can be contacted using:

Address : Peter Sloman
Data Protection Officer
Weston College
Knightstone Campus
Weston-super-Mare
BS23 2AL

Email : data.protection@weston.ac.uk
Telephone : 01934 411411

5 PERSONAL DATA

5.1 Any combination of data items that could identify a living person and provide specific information about them, their families or circumstances. The term covers both facts and opinions about an individual. Weston College Group may process a wide range of personal data of staff (including governors and volunteers) learners, their parents or guardians as part of its operation.

5.2 This personal data may include (but is not limited to):

- Names and addresses (including email addresses)
- Bank details
- Academic data e.g. progress records, disciplinary actions, admissions and attendance records
- References
- Employment history
- Taxation and national insurance records

- Appraisal records
- Examination scripts and marks

6 SPECIAL CATEGORY PERSONAL DATA

6.1 Special category personal data - Personal data which is more sensitive and so needs more protection, including information about a living individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns, voice biometrics), used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

6.2 We maintain a Record of Processing Activities (RoPA) which details the types of information we hold and the grounds upon which we process it, as does our Privacy Notice which may be found at www.weston.ac.uk/dataprivacy.

6.3 Examples of the types of special category data we hold may be found in Appendix 1.

7 SUBJECT ACCESS REQUESTS & OTHER RIGHTS

7.1 The Data Protection Officer (DPO) is responsible for advising on the implementation of this policy, monitoring

7.2 In all aspects of its work, Weston College Group will ensure that the rights of the data subject are protected by all practicable measures associated with the conduct of Weston College Group's work. Subject to exceptions, the rights of the data subject as defined in law are:

a) The Right to be informed.

7.2.1 Weston College Group advises individuals how it will use their data through the use of transparent Privacy Notices and other documentation, such as data capture and consent forms where appropriate.

b) The Right of access

7.2.2 An individual when making a subject access request (SAR) is entitled to the following;

i. Confirmation that their data is being processed;
ii. Access to their personal data;
iii. Other supplementary information – this largely corresponds to the information that should be provided in a Privacy Notice.

7.2.3 Weston College Group must respond to such a request within one calendar month unless the request is complex, in which case it may be extended by a further 2 calendar months. Please refer to Appendix 2 for further details as to how to manage a subject access request.

c) The Right to rectification

7.2.4 Individuals have the right to ask us to rectify information that they think is inaccurate or incomplete. Weston College Group must investigate any such claims and rectify the information where appropriate within one calendar month, unless an extension of up to a further 2 calendar months can be justified.

d) The Right to erasure

7.2.5 Individuals have a right to request that their personal information is erased but this is not an absolute right. It applies in circumstances including where:

- The information was given voluntarily, consent is now withdrawn and no other legal basis for retaining the information applies;
- The information is no longer required by Weston College Group;
- A legal obligation to erase the data applies;
- The data was collected from a child for an online service or
- Weston College Group has processed the data on the basis that it is in their legitimate business interests to do so and having conducted a legitimate interests test, it concludes that the rights of the individual to have the data erased outweigh those of Weston College Group to continue to process it.

7.2.6 Weston College Group will consider such requests as soon as possible and within one month unless it is necessary to extend that timeframe for a further two months based if the complexity of the request or numerous requests has been received from the same individual.

e) The Right to restrict processing

7.2.7 This is not an absolute right. An individual may ask Weston College Group to temporarily limit the use of their data (for example store it but not use it) when it is considering:

- A challenge made to the accuracy of their data, or
- An objection to the use of their data.

7.2.8 In addition, Weston College Group may be asked to limit the use of data rather than delete it:

- If the individual does not want Weston College Group to delete the data but does not wish to it continue to use it;
- If the data was processed without a lawful basis;
- To create, exercise or defend legal claims.

f) The Right to data portability

7.2.9 An individual can submit a request concerning data that is held electronically for it to be transferred to another organisation or to themselves where they have provided it either directly or through monitoring activities e.g. apps. Weston College Group only has to provide the information where it is electronically feasible.

g) The Right to object

7.2.10 Individuals have a right to object to the processing of their data in regards to:

- a task carried out in the public interest except where personal data is processed for historical research purposes or statistical purposes
- a task carried out in its legitimate interests
- scientific or historical research, or statistical purposes, or
- direct marketing.

7.2.11 Only the right to object to direct marketing is absolute, other objections will be assessed following the data protection principles. Weston College Group will advise of any decision to refuse such a request within one month, together with reasons and details of how to complain and seek redress.

h) Rights related to automated decision making

7.2.12 This does not apply as Weston College Group does not employ automated decision-making processes.

8 DATA PROTECTION PRINCIPLES

8.1 The GDPR is based on 7 key data protection principles that Weston College Group complies with.

8.2 The principles say that personal data must be:

Processed lawfully, fairly and in a transparent manner

8.3 Weston College Group will explain to individuals why Weston College Group needs their data and why it is processing it – for example on consent forms (where consent is used as the basis for processing), and in its Privacy Notice(s). Weston College Group reviews its documentation and the basis for processing data regularly

Collected for specified, explicit and legitimate purposes

8.4 Weston College Group explains these reasons to the individuals concerned when it first collects their data. If Weston College Group wishes to use personal data for reasons other than those given when the data was first obtained, it will inform the individuals concerned before doing so and will seek consent where necessary and appropriate unless the new purpose is compatible with that in respect of which consent was given, or there is another lawful basis for sharing the information/ Weston College Group will document the basis for processing.

Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

8.5 Weston College Group must only process the minimum amount of personal data that is necessary to undertake its work.

Accurate and, where necessary, kept up to date

8.6 Weston College Group will check the details of those on its databases at appropriate intervals and maintain the databases. It will consider and respond to requests for inaccurate data to be rectified following the Data Protection Act 2018.

Kept for no longer than is necessary for the purposes for which it is processed

8.7 We review what data we hold at appropriate intervals – for example upon the annual review of the Record of Processing Activities (or sooner if needed).

8.8 When Weston College Group no longer needs the personal data it holds, it will ensure that it is deleted or anonymised following the Weston College retention policy and schedule. We only keep personal data, including special category data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where there is a legal obligation to do so

8.9 We have a retention and disposal policy that governs how long all data including special category data shall be retained. The retention policy and schedule is reviewed regularly;

8.10 Once the data is no longer needed, we delete it, securely destroy it in line with our ISMS Control of Information Assets Policy or we will render it permanently anonymous.

Processed in a way that ensures it is appropriately secure

8.11 Weston College Group implements appropriate technical measures to ensure the security of data and systems for staff and all users.

8.12 Weston College Group have an Information Security Management Systems (ISMS) which is certified to ISO 27001

8.13 Please refer to the IT Acceptable User Policy & eSafety and Social Media Policy for further information which incorporates principles around Bring Your Own Device (BYOD), Weston College Groups home working policy and how data is securely transferred in and out of our IT systems.

8.14 Weston College Group defines the security methods of data transfer within is ISMS Control of Information Assets Procedure which is part of the Weston College Information Security Management System (ISMS). The ISMS is reviewed and audited as part of the Weston College ISO 27001 Certification

Accountability

8.15 Weston College Group complies with its obligations under data protection laws including the GDPR and can demonstrate this via the measures set out in this policy including:

8.15.1 Completing Data Protection Impact Assessments (DPIAs) where Weston College Group's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies. This largely involves special category personal data and CCTV. However, Weston College Group will liaise with the DPO who will advise on this process. Any activity involving the processing of personal data must be registered on the Register of Processing Activity and reviewed, at the very least, annually;

8.15.2 Integrating data protection into internal documents including this policy, any related policies and Privacy Notices;

8.15.3 Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; Weston College Group also maintains a record of attendance; Staff who process special category data will be provided with such additional training as appropriate for example on safeguarding systems. Records of training are maintained;

8.15.4 Regularly conducting reviews and audits to test its privacy measures and ensure compliance with relevant legislation and school policies;

8.15.5 Maintaining records of its processing activities for all personal data that it holds;

8.15.6 Policies related to the handling of data and associated documentation will be regularly reviewed on a rolling basis and updated following any new guidance, legislation and practice.

8.15.7 The Record of Processing Activities is a working document that will be maintained and reviewed regularly;

8.15.8 Where any breaches of personal data have occurred, the reasons for this will be reviewed and changes made to practice and procedure as appropriate;

8.15.9 Stakeholders will manage risks and compliance using the annual compliance statement provided by the Data Protection Officer and/or a Risk Register.

9 PROCESSING PERSONAL DATA

9.1 To ensure that Weston College Group's processing of personal data is lawful; it will always identify one of the following six grounds for processing **before** starting the processing:

9.1.1 The data needs to be processed so that Weston College Group can fulfil a **contract** with the individual, or the individual has asked Weston College Group to take specific steps before entering into a contract;

9.1.2 The data needs to be processed so that Weston College Group can comply with a **legal obligation**;

9.1.3 The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life;

9.1.4 The data needs to be processed so that Weston College Group, as a public authority, can **perform a task in the public interest, and carry out its official functions**;

9.1.5 The data needs to be processed for the **legitimate interests** of Weston College Group or a third party where necessary, balancing the rights or freedoms of the individual).

9.1.6 However, where Weston College Group can use the **public task** basis for processing, it will do so rather than rely on legitimate interests as the basis for processing.

9.1.7 The individual (or their parent/carer when appropriate in the case of learners) has freely given clear consent. In the case of **special categories of personal data**, this must be **explicit consent.** Weston College Group will seek consent to process data from the learner or parent/guardian depending on their age and capacity to understand what is being asked for.

9.2 In addition to the legal basis to process personal data, special categories of personal data also require an additional condition for processing under Article 9 of the GDPR. The grounds that we may rely on include:

9.2.1 The individual has given **explicit consent** to the processing of those special categories of personal data for one or more specified purposes;

9.2.2 The processing is necessary for carrying out the obligations and exercising specific rights under **employment, health and social security and social protection law and research**; a full list can be found in Schedule 1 Part 1 of the Data Protection Act 2018.

Health or social care purposes includes the following purposes:

i. Preventative or occupational medicine
ii. The assessment of the working capacity of the employee

9.2.3 The processing is necessary to protect the **vital interests** of the individual or of another natural person where the individual is physically or legally incapable of giving consent;

9.2.4 The processing relates to personal data which are manifestly **made public** by the individual;

9.2.5 The processing is necessary for the **establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity;

9.2.6 The processing is necessary for reasons of **substantial public interest** but must be demonstrated and assessed as part of the public interest test and evidenced throughout the decision-making process.

These grounds include the following (the full list of defined purposes may be found in Schedule 1 Part 2 of the Data Protection Act 2018):

- Statutory and government purposes
- Safeguarding of children or individuals at risk
- Legal claims
- Equality of opportunity or treatment
- Counselling
- Occupational pensions

9.2.7 The processing is necessary for preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services based on Union or Member State law or under contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3

9.2.8 The processing is necessary for reasons of **public interest in the area of public health**;

9.2.9 The processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.**

9.3 Deciding upon the correct legal basis for processing data can be difficult and more than one ground may be applicable. We consult with the Data Protection Officer where appropriate.

9.4 We must also comply with Schedule 1 of the Data Protection Act (as well as Articles 6 and Article 9) when we are processing data where the conditions relating to employment, health and research or substantial public interest are as follows:

Legal basis for processing criminal offence data

9.5 Criminal offence data includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions.

9.6 We do not maintain a register of criminal convictions.

9.7 When processing this type of data, we are most likely to rely on one of the following bases:

9.7.1 The processing is necessary for performing or exercising obligations or rights which are imposed or conferred by law on the controller or the individual in connection with employment, social security or social protection; or

9.7.2 Consent – where freely given. The School acknowledges because of the potential for the imbalance of power that it may be difficult for consent to be deemed valid and will only rely on this where no other ground applies.

10 SHARING PERSONAL DATA

10.1 Please refer to Weston College Group Privacy Notice(s).

10.2 Weston College Group will only share personal data under limited circumstances when there is a lawful basis to do so and where identified in the Privacy Notice(s). The following principles apply:

10.2.1 Weston College Group will share data if there is an issue with a learner or a third party, for example, parent/carer that puts the safety of staff or others at risk;

10.2.2 Weston College Group will share data where there is a need to liaise with other agencies. It will seek consent as necessary and appropriate before doing so. However, where child protection and safeguarding concerns apply, it will apply the “Seven golden rules of information sharing” which provide that in limited circumstances data may be shared with external agencies without the knowledge or consent of the parent or learner;

10.2.3 Weston College Group suppliers and contractors including its data protection officer and IT Department may need data to provide services. When sharing data, Weston College Group will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
- Establish a data processing contract 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 it shares where there is regular sharing;
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with Weston College Group.

10.3 Weston College Group may also share personal data with law enforcement and government bodies where there is a lawful requirement/basis for us to do so, including:

- For the prevention or detection of crime and/or fraud;
- For the apprehension or prosecution of offenders;
- For the assessment or collection of tax owed to HMRC;
- In connection with legal proceedings;
- For research and statistical purposes, if personal data is sufficiently anonymised, or consent has been provided.

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

11 DATA PROTECTION BY DESIGN

11.1 Weston College Group has a legal obligation to integrate appropriate technical and organisational measures into all its processing activities and to consider this aspect before embarking on any new type of processing activity.

11.2 Weston College Group completes a Data Protection Impact Assessment (DPIA) for any activity which may involve a high risk to the data protection rights of the individual.

11.3 Weston College Group have an Information Security Management Systems (ISMS) which is certified to ISO 27001

12 PERSONAL DATA BREACHES

12.1 A personal data breach is defined as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service.” It may be deliberate or accidental.

12.2 Wherever it is believed that a security incident has occurred or a ‘near miss’ has occurred, the staff member must inform the IT Helpdesk and/or the Data Protection Officer immediately so that an assessment can be made as to whether the ICO should be informed within 72 hours as is legally required, and/or those data subjects affected by the breach.

12.3 Incidents are reported and tracked via the College’s Information Security Management Systems (ISMS) following the ISMS Incident Management Procedure.

12.4 Weston College will work closely with the ICO and follow the ICO guidance in regards to any personal data breaches

12.5 If you would like to report an Information Security incident please email data.protection@weston.ac.uk

13 BIOMETRIC RECOGNITION SYSTEMS

Biometric data consists of personal information about an individual's physical or behavioural characteristics which may be used to identify that person. It may take the form of fingerprint, voice or facial recognition. We use biometric in the following ways

- Some IT devices use face or fingerprint biometrics data to simplify the authentication process (this is by explicit consent and you may use a traditional password / PIN as an alternative)

13.1 We will undertake a data protection impact assessment before implementing any new biometric system to assess the impact on individuals.

13.2 We will seek their consent direct from them before processing any biometric data.

13.3 If the individual concerned does not agree to proceed or wishes to withdraw their consent to the use of the biometric system, we will provide an alternative means of achieving the same aim.

14 DESTRUCTION OF RECORDS

14.1 Weston College Group adheres to its retention policy and will permanently securely destroy both paper and electronic records following these timeframes.

14.2 Weston College Group will ensure that any third party who is employed to perform this function has the necessary accreditations and safeguards.

14.3 Where Weston College Group deletes electronic records and it intends to put them beyond use, even though it may be technically possible to retrieve them, it will follow the Information Commissioner's Code of Practice on deleting data and this information will not be made available on receipt of a subject access request.

15 TRAINING

15.1 To meet its obligations under Data Protection legislation, Weston College Group ensures that all staff, volunteers, and Governors receive data protection training as part of their induction. Those who need additional training will be provided with it, for example relating to the use of systems or as appropriate, at least every two years

15.2 Data protection also forms part of continuing professional development, and updates will be provided where changes to legislation, guidance or Weston College Group's processes make it necessary.

16 MONITORING ARRANGEMENTS

16.1 Whilst the DPO is responsible for advising on the implementation of this policy and monitoring Weston College Groups overall compliance with data protection law, Weston College Group is responsible for the day to day implementation of the policy and for making the data protection officer aware of relevant issues which may affect Weston College Group ability to comply with this policy and the legislation.

16.2 This policy will be reviewed annually unless an incident or change to regulations dictates a sooner review.

17 COMPLAINTS

17.1 We take any complaints about our handling of personal information very seriously.

17.2 If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please use the contact details below to let us know

17.3 If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please use the contact information below

Address : Peter Sloman
Data Protection Officer
Weston College
Knightstone Campus
Weston-super-Mare
BS23 2AL

Email : data.protection@weston.ac.uk
Telephone : 01934 411411

17.4 You can also complain to the ICO if you are unhappy with how we have used your data, but they would generally expect you to have raised the issue with us first. The ICO's address:

Address : Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone : 0303 123 1113
ICO website : https://www.ico.org.uk

18 TERMS & DEFINITIONS

18.1 **Processing** - Anything that is 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.

18.2 **Data subject** - The identified or identifiable (living) individual whose personal data is held or processed.

18.3 **Data controller** - A person or organisation that determines the purposes and the means of the processing of personal data.

18.4 **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.

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

18.6 **DPA:** - Data Protection Act 2018 – Law that controls how your personal information is used by organisations, businesses or the government

18.7 **GDPR:** - EU General Data Protection Regulation 2018 - a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU)

18.8 **ICO:** - Information Commissioner Office - The ICO is the UK's independent body set up to uphold information rights. Find out more about our organisation and structure.

18.9 **SAR:** - Subject Access Request – Individuals have the right to request a copy of any information

19 COMPLIANCE MONITORING & REVIEW

19.1 This document will be reviewed annually by the Weston College Group's Data Privacy Management Group (DPMG)

19.2 The Weston College Group's Data Privacy Management Group (DPMG) is responsible for the management of this document reporting to the College Leadership Board & the Governing Body.

19.3 This policy will be maintained as part of the Information Security Management System (ISMS) as part of the College ISO 27001 certification

20 RELATED LEGISLATION AND DOCUMENTS

20.1 Legislation

- Data Protection Act 2018
- UK General Data Protection Regulation 2020
- Privacy and Electronic Communications Regulations (PECR) 2003

20.2 WCG Policies:

- Freedom of Information Policy
- Information Security Policy
- Record of Processing Activities

APPENDIX 1 – EXAMPLES OF SPECIAL CATEGORY DATA WE PROCESS

Examples of where we may process special category data include:

- Accident reporting documentation
- Attendance records
- Biometric data
- Disciplinary and Capability proceedings
- Disclosure and Barring Service (DBS)
- Equal Opportunities data (disability, race, ethnicity, sexual orientation).
- Health data
- Right to work data
- Safeguarding records

Our Record of Processing Activities (RoPA) details the types of information we hold and the grounds upon which we process it, as does our Privacy Notice which may be found at www.weston.ac.uk/dataprivacy.

APPENDIX 2 – SUBJECT ACCESS REQUEST (SAR) PROCEDURE

Weston College Group shall complete the following steps when processing a request for personal data (Subject Access Request or SAR).

1. Ascertain whether the requester has a right to access the information and capacity.

2. Obtain proof of identity (once this step has been completed the clock can start)

3. Engage with the requester if the request is too broad or needs clarifying

4. Make a judgement on whether the request is complex and therefore can be extended by an additional 2 months

5. Acknowledge the requester providing them with
    a. the response time – 1 month (as standard), an additional 2 months if complex; and
    b. details of any costs – Free for standard requests, or you can charge, or refuse to process if the request is manifestly unfounded or excessive, or further copies of the same information is required, the fee must be in line with the administrative cost

6. Use its Record of Processing Activities and/or data map to identify data sources and where they are held

7. Collect the data (the organisation may use its IT support to pull together data sources – for access to emails the organisation can do so as long as it has told staff it will do so in its policies)

8. If (6) identifies third parties who process it, then engage with them to release the data to Weston College Group.

9. Review the identified data for exemptions and redactions in line with the ICO's Code of Practice on Subject Access

10. Create the final bundle and check to ensure all redactions have been applied

11. Submit the final bundle to the requester in a secure manner and in the format they have requested.