Data Protection and Information Security Policy

Richard Huish College

Senior Management Team

Approved by the RHC SMT:	May 2021
Approved by the Audit Committee:	May 2021
Next review due by:	May 2022

Contents

Data Protection and Information Security Policy

Introduction and Aims

The College aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

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

1. Legislation and guidance

This policy meets the requirements of the GDPR and 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 meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data (if applicable).

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 agreement and Instrument and Articles of Government.

2. 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.

3. The Data Controller

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

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

4. Roles and responsibilities

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

4.1 Board of Governors

The Board of Governors has overall responsibility for ensuring that our College complies with all relevant data protection obligations.

4.2 Data Protection Officer (DPO – see Appendix 1)

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 Board of Governors and, where relevant, report to the Board their advice and recommendations on College data protection issues.

.

Full details of the DPO's responsibilities are set out in their job description in **Appendix 1.**

Our DPO is Amy Brittan College Data Protection Officer and is contactable via dpoAcademys@somerset.gov.uk

4.3 Principal or CEO

The Principal or CEO acts as the representative of the data controller on a day-to-day basis.

4.4 Data Protection Leads (DPL – see Appendix 1)

The College has a named individual Data Protection Lead (DPL), Sarah Hughes Email: sarahh@richuish.ac.uk

The DPL is the first point of contact for individuals whose data the College processes, and for the ICO

The DPL's responsibilities include but are not limited to:

- recording DP training for all staff
- ensuring staff are aware of the DP Policy and the Personal Data Breach procedure
- recording all Subject Access Requests and the completion timeliness
- recording all data breaches and working with the DPO to mitigate against this happening again
- completing an annual online DP assessment to monitor compliance and produce a report for the Board of Governors.

4.5 All staff

All staff are responsible for checking that any information that they provide to the College is accurate and up to date.

All staff are responsible for ensuring that any personal data they use in the process of completing their role:

- is not in the view of others who do not have the authority to view the data;
- is kept securely in a locked cabinet when not being used;
- is stored on a secure local or network drive;
- if kept on removable storage (laptop, tablet, USB memory stick) approved by the College, that this is password protected and encrypted. The data held on these devices must be backed up regularly and this is the responsibility of the individual;
- is not disclosed to any unauthorised third party;
- is assessed through a Privacy Impact Assessment (PIA) if the DPL and DPO judge it to be necessary

Staff should note that unauthorised disclosure or transgression of the above statements may be a disciplinary matter.

Staff should contact the DPL 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 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

4.6 Responsibilities of Parents/Guardians

The College will inform the Parents/Guardians of the importance of the personal data the College uses and the importance of keeping this up to date. This process will include at least an annual data collection sheet (with the return of this document being recorded) and reminders in newsletters and at tutor or class meetings.

Other permissions will also be sought regarding matters of non-statutory use of personal data such as the use of images and names in publicity materials on induction or when required. The returns to these permissions will be recorded and exemptions communicated to staff.

5. Data protection principles

The GDPR is based on data protection principles that the 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 the College aims to comply with these principles.

6. Collecting personal data

6.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under Article 6 of the General Data Protection Regulation:

- The data needs to be processed so that the College can **fulfil a contract** with the individual, or the individual has asked the College to take specific steps before entering into a contract
- The data needs to be processed so that the 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 the 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 the 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 student) has freely given clear **consent**

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

We will seek to use the legal basis of legitimate interests (Article 61(f)) for the online services we use for teaching and learning. We will apply the 'three-part test' to ensure we can use this as our legal basis. If we cannot use legitimate interests as our legal basis, we will rely on consent (Article 6 1 (a)) as a basis for processing and we will get parental consent (except for online counselling and preventive services). Consent will be specific, informed and verifiable and can be withdrawn at any time.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law though our Privacy Policy and information included on data collection forms.

6.2 Limitation, minimisation and accuracy

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

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we 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 in accordance with the IRMS toolkit for schools. Information and Records Management Society's toolkit for Academies .

7. Sharing personal data

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

- There is an issue with a student or parent/carer that puts the safety of the student or our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we 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 we 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
    - complete a Privacy Impact Assessment (PIA) to assess the risk of data loss from breach or mismanagement, and the necessary steps to minimise risk

We will also share personal data with law enforcement and government bodies where we 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

We 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 students or staff.

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

8. Subject access requests and other rights of individuals

8.1 Subject access requests

All people having personal data stored by the College have the rights to:

a) obtain from the College confirmation if personal data concerning him or her (or their child) is being processed;

b) Where this is the case, have a copy of the personal data and the following information:

(i) the purposes of the processing;

(ii) the third parties that the data will be shared with;

(iii) the period for which the personal data will be stored;

(iv) the existence of the right to request from the College to correct, erase or restrict processing of personal data if the data can be proved to be incorrectly held;

(v) the right to lodge a complaint with a supervisory authority;

(vi) where the personal data are not collected from the data subject, any available information as to their source.

c) if exemptions are placed on any of the data above, because of safeguarding or other issues, the existence of this data will be declared.

The College will place on its website the College's Privacy Notices[1] regarding the personal data held about them and the reasons for which it is processed.

Access to the data is called a Subject Access Request. Any person who wishes to exercise this right (or their parental right) should make a request in writing and submit it to the Principal or the Board of Governors.

8.2 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 students at our College may not be granted without the express permission of the student This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

8.3 Responding to subject access requests

When responding to requests, we will follow the procedure laid out in **Appendix 2.**

[1] https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

When a subject access request is received by the College the DPL and DPO will complete a Subject Access Request form for the College's documentation **(see Appendix 3)**

8.4 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 we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- withdraw their consent to processing 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 DPL. If staff receive such a request, they must immediately forward it to the DLP.

9. Parental requests to see the educational record

While the College is exempt from legislation to provide an educational record, we will endeavour to provide this information to parents. Parents, or those with parental responsibility, are able to request access to their child's educational record (which includes most information about a student), by making a request in writing to the Data Protection Lead. The College will deal with this request as a Subject Access Request and provide the information within one calendar month.

10. Freedom of Information Requests

Freedom of Information requests are requests from any member of the public about processes, policies and other non-personal information a public authority. These requests will always be processed and the rights of individuals (within Data Protection Act 2018) not to be identified respected while maintaining legal responsibilities within the Freedom of Information Act 2000.

For further information on our Freedom of Information procedures, please see our College Freedom of Information policy.

11. CCTV

For further information about our CCTV procedures, please see our CCTV code of practice.

We use CCTV in various locations around the College site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV and advice from the Surveillance Commissioner.

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

CCTV images can be supplied to the data subject on request and will be treated as a subject access request.

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

12. Photographs and videos

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

Some photos may be used around the College site on display boards to celebrate learning e.g. photos from recent events or productions. We will not seek consent from the students for these photos to be displayed and will rely on the legal basis of Article 6 1 (f) of GDPR: legitimate interests. The student can use their right to object to the data being processed (photo on display) at any time.

Consent for taking photographs will be from the student using Student Advantage. A student can change their preferences at any time so it is advised to check permissions each time you take/use a photograph.

Students who have not provided consent to have their photograph taken or be filmed will have their wishes respected. If a student changes their consent preferences all references to them should be removed immediately you are aware of the change of consent wherever possible. With printed publications, the images should be removed when the document is next updated.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials or uses beyond the physical site of the College.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student.

Uses where we may seek consent may include:

- In College magazines, brochures, newsletters, etc.
- Outside of College by external agencies such as the College photographer, newspapers, campaigns
- Online on our College website or social media pages

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

When using photographs and videos in this way we will not accompany them with any other personal information about the student, to ensure they cannot be identified.

Photos will be securely disposed of once the child ceases to be a student at the College. A small number of photos may be kept for the College's historical record but will be stored securely.

See our College Acceptable Use Policy for more information on our use of photographs and videos.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our 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 (PIAs) where the 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; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our College and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

We 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 the College office
- Passwords that are at least 8 characters long are used to access College computers, laptops and other electronic devices.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for College-owned equipment (see our acceptable use policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Retention and Disposal of records

Records Management is the process by which the College manages all aspects of any type of 'record' whether internally or externally generated and in any format or media type, from their creation, throughout their lifecycle and to their eventual disposal.

15.1. Relevant Data Protection Principles

The data protection principles which directly relate to the management, retention and disposal of Personal Data are that the Personal Data must:

I. be accurate and kept up to date (Principle 4)

II. not be kept longer than necessary for the purpose for which it was obtained (Principle 5)

III. be processed by a Data Controller who has in place appropriate technical and organisational measures to prevent unauthorised processing and accidental loss, destruction or damage (Principle 7).

15.2 Retention Periods

In line with the fifth principle as set out at 17.1 (ii) above the College will not retain Data any longer than necessary and in determining an appropriate retention period will consider the following:

I. The current and future value of the Data.

II. The costs, risks and liabilities associated with retaining the Data.

III. The ease or difficulty in ensuring the Data remains accurate and up-to-date.

The standard default period for retaining Data will be based on the Information and Records Management Society's toolkit for Academies produced by the Records Management Society. The retention schedule for the main types of data we hold within the College are set out in **Appendix 6.** A more comprehensive list can be seen in the toolkit.

15.3 Exceptions to the Retention Period

In the majority of cases Data will be securely disposed of when it reaches the end of the retention period. When assessing whether Data should be retained beyond the retention period the College will consider whether:

- The Data is subject to a request pursuant to the DPA.
- The College is the subject of or involved in ongoing legal action to which the Data is or may be relevant.
- The Data is or could be needed in connection with an ongoing investigation.
- There is a greater public interest in retaining the Data.
- There are changes to the regulatory or statutory framework.

15.4 Disposal of Data

The destruction of Data is an irreversible act and must be clearly documented. All Data identified for disposal will be destroyed under confidential conditions.

The College may sub-contract to another organisation its obligations to dispose of Data under confidential conditions. Where the obligation to securely dispose of Data is sub-contracted, the College will satisfy itself of the subcontractor/third party's experience and competence to do so.

15.5 Manual Records

Where Data is held in paper or other manual form, the retention period has expired and none of the exceptions for retaining Data beyond the retention period as set out at paragraph 17.3 is satisfied, the College will ensure the Data is shredded or otherwise confidentially disposed of.

15.6 Electronic Records

Where Data is held in an electronic format the College will, where feasible, use its reasonable endeavours to:

I. Surround the Data with such technical and security measures to ensure it is not accessible other than by a Data Processor.

When the data is no longer required:

II. Put the Data beyond use so that the Data is no longer on a live electronic system and cannot be accessed by its own employees (with the exception of IT support) or a Data Processor.

III. Permanently delete the Data from the College electronic systems when and where this becomes possible.

Where the steps set out at paragraph 17.7.ii are complied with, the College considers the Data to be 'put beyond use' and this Data will not be used in order to respond to a Subject Access Request.

16. Personal data breaches

The College will make all reasonable endeavours to ensure that there are no personal data breaches.

The procedure for dealing with a data breach is laid out in **Appendix 5.**

All Data Breaches will be recorded, comprising the facts relating to the personal data breach, its effects and the remedial action. The proforma for recording data breaches is in **Appendix 6.**

If there are risks to the individual the College will communicate the breach to the data subjects and inform the ICO **within 72 hours of notification**. Breaches that may require escalation to the ICO may include but are not limited to:

- A non-anonymised dataset being published.
- Safeguarding information being made available to an unauthorised person.
- The theft of a Collegelaptop containing non-encrypted personal data about students.

Further investigation of the breach can take place after this notification in line with advice from the DPO and the ICO.

Data breaches are reported using the information found at his webpage: https://ico.org.uk/for-organisations/report-a-breach/ and https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

When reporting a breach, the Data Protection Act 2018 states that we must provide:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

17. Training

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

Data Protection procedures are part of the College's Code of Conduct and Acceptable User Policy,

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

18. Monitoring arrangements

The DPL in conjunction with the DPO is responsible for monitoring and reviewing this policy.

19. Links with other policies

This data protection policy is linked to our:

- RHC Privacy Notices for Parents/Carers, Students, Workforce and Governance
- RHC Acceptable Use Policy
- RHC Code of Conduct
- RHC Freedom of information publication scheme
- CCTV Code of Practice

Appendix 1: The roles of the Data Protection Officer and Data Protection Leads

Purpose

The Data Protection Officer (DPO) is responsible for monitoring compliance with current data protection law, and has the knowledge, support and authority to do so effectively. They oversee and verify the College's data protection processes and advise the College on best practice.

The College Data Protection Lead (DPL) is Sarah Hughes, who maintains contact with the DPO and is responsible for assisting in monitoring with compliance and verifies the College's data protection practices on a day to day basis.

Data Protection Officer Responsibilities

To:

- verify that the College has registered with the ICO;
- advise the College about their obligations under the Data Protection Act 2018;
- support the College DPL in developing a joint understanding of the College's processing operations, information systems, data security processes and needs, and administrative rules and procedures;
- assist, in cooperation with the DPL, with the monitoring of the College's compliance with data protection law, by:
    - collecting information to identify data processing activities;
    - analysing and checking the compliance of data processing activities;
    - informing, advising and issuing recommendations to the College;
    - ensuring they have current and detailed information in data protection issues and changes to the law, attending relevant training as appropriate;
- assist the DPL in making sure that the College's policies are followed, through:
    - assigning responsibilities to individuals;
    - awareness-raising activities;
    - coordinating staff training;
    - conducting internal data protection audits;
- advise on and assist the College with carrying out data protection privacy impact assessments, if necessary;
- act as a contact point for the ICO, assisting and consulting it where necessary, including:
    - helping the ICO to access documents and information;
    - seeking advice on data protection issues;
- act as a contact point for individuals whose data is processed (for example, staff, students and parents), including:
    - responding with support from the DPL to subject access requests;
    - responding with support from the DPL to other requests regarding individuals' rights over their data and how it is used;
- take a risk-based approach to data protection, including:
    - prioritising the higher-risk areas of data protection and focusing mostly on these
    - advising the College if/when it should conduct an audit, which areas staff need training in, and what the DPO/DPL roles should involve.

- report to the Board of Governors on the College's data protection compliance and associated risks;
- respect and uphold confidentiality, as appropriate and in line with data protection law, in carrying out all duties of the role;
- assist the DPL in maintaining a record of the Colege's data processing activities;
- work with external stakeholders, such as suppliers or members of the community, on data protection issues;
- working with the DPL to build a culture of data protection throughout the College;
- work closely with other departments and services to ensure GDPR compliance, such as HR, legal, IT and security;
- work with the Senior Leadership team at the College to ensure GDPR compliance;
- assist with any additional tasks necessary to keep the College compliant with data protection law and be successful in the role.

Tasks

From these responsibilities, isolated tasks should include:

- providing a model Data Protection Policy and assist in customising it for the College;
- advising on procedures and pro formas to allow the Data Protection Policy to be adhered to;
- providing advice on other associated policies and documents;
- providing materials and advice in completing a dynamic Data Asset Audit and assisting in its completion if necessary;
- checking issues with the Data Asset Audit;
- providing training materials to allow the DPL to assist staff in keeping up to date with Data Protection issues;
- acting as the point of contact for SAR and FOI requests and supporting the College to provide the information as required;
- providing a Data Protection Audit on a 3 yearly rota basis and producing a report for Governors at cost;
- providing telephone and email advice and support;
- providing regional training for the DPL and other staff;
- providing College based on-demand training at cost.

Data Protection Lead Responsibilities

To:

- support the DPO in advising the College about their obligations under the Data Protection Act 2018;
- support the DPO in developing an understanding of the College's processing operations, information systems, data security processes and needs, and administrative rules and procedures;
- assist, in cooperation with the DPO, with the monitoring of the College's compliance with data protection law, by:
    - collecting information to identify data processing activities;

    - analysing and checking the compliance of data processing activities;
    - informing, advising and issuing recommendations to the College;
    - ensuring they have current and detailed information in data protection issues and changes to the law, attending relevant training as appropriate;
- assist the DPO in making sure that the College's policies are followed, through:
    - assigning responsibilities to individuals;
    - awareness-raising activities;
    - coordinating staff training;
    - conducting internal data protection audits;
- act as a contact point for the DPO in supporting individuals whose data is processed (for example, staff, students and parents), including:
    - responding with support from the DPO to subject access requests;
    - responding with support from the DPO to other requests regarding individuals' rights over their data and how it is used;
- assist the DPO in maintaining a record of the College's data processing activities providing this on a yearly basis to the DPO;
- assisting the DPO in working with external stakeholders, such as suppliers or members of the community, on data protection issues;
- working with the DPO to build a culture of data protection throughout the College;
- work with the Senior Leadership team at the College to ensure GDPR compliance;
- assist with any additional tasks necessary to keep the College compliant with data protection law and be successful in the role.

Tasks

From these responsibilities, isolated tasks should include:

- act as the point of contact with the DPO for data breaches and subject access requests
- receiving and reading the DPO's monthly newsletter and identifying issues that could affect the College;
- advising on procedures and pro formas to allow the Data Protection Policy to be adhered to;
- provide advice on other associated policies and documents;
- providing materials and advice in completing a Data Asset Audit and assisting in its completion if necessary;
- supplying the DPO with the Data Asset Audit on a yearly basis;
- using the training materials provided by the DPO to assist the staff in keeping up to date with Data Protection issues.

Appendix 2: Process for dealing with a subject access request

On receiving a Subject Access Request or request for change or deletion of data the DPO Or College will:

- inform the DPL in the College (and the Principal if necessary);
- record the details of the request, updating this record where necessary **(see Appendix 3)**
- reply to the requestor informing receipt of the request asking for clarity if there is confusion about which data is required
- contact the DPO if clarity on the request is needed or procedure is needed;
- identify the people responsible for gathering the necessary data;
- gather the data indicating a deadline;
- examine the data for redactions making sure there is no 'bleeding' of data;
- ask the requestor for an address and time for delivery.

The whole process should take no longer than **30 calendar days**, which can be extended by a further 2 months where the request is complex or where there are numerous requests.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the 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

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers 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 we refuse a request, we will tell the individual why, and tell them they have the right to complain to the Information Commissioners Office (ICO).

Appendix 3: Subject Access Request Record

Name of data subject: _____

Name of person who made request: _____

Date request received: ____/____/____

Contact DPO (dposchools@somerset.gov.uk) : ____/____/____

Date acknowledgement sent: ____/____ /____

Name of person dealing with request: _____

	Notes (Overwrite the instructions in grey italics)
Are they entitled to the data?	If no reply stating reasons and/or ask for proof
Do you understand what data they are asking for?	If no, ask requestor for clarity
Identify the data	What data sources, where they are kept
Collect the data required	You may need to ask others – state a deadline in your request.
Do you own all the data?	If no, ask third parties to release external data. If data is supplied by another agency such as Psychology Service, you do not own the data.
Do you need to exempt/redact data?	If exempting/redacting be clear of your reasons Document name, data exempted/redacted, why.
Is the data going to be ready in time?	Record delays and reasons. Communicate with requestor stating reason for delay and asking if they would like the data you have collected so far.
Create pack	Make sure that the data is in an easy to access format: paper, word, excel etc.
Inform requestor you have the data	Ask them how they would like it delivered
Deliver data	Ask for confirmation/special delivery?

Date request completed: ____/____/____

(within 30 days of request)

Signed off by: _____

Appendix 4: Data Retention Schedule

The following retention schedule is in operation. This lays down the length of time a record needs to be retained, after which it will be destroyed. Time scales are based on local Government guidelines.

Students	Students' academic records reports and IEPs	DOB of pupil + 25 years (records moved from Primary to Secondary Academy)
	Students attendance registers	Date of register + 3 years
	Exam results (internal & external)	Added to student file
	Statements of Special Needs	DOB + 30 years
	Child Protection Information	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period as the pupil file.
	Timetable	Current Year + 1 Year
	Syllabus	Current Year + 1 Year
	Markbooks	Current Year + 1 Year
	Students work*	Current Year + 1 Year *It may necessary to extend this period for examination
Personnel	Staff Personnel Files	Termination of employment + 6 years
	Records leading to appointment of a new Principal	Date of appointment + 6 years
	Records leading to appointment of a new member of staff (unsuccessful candidates)	Date of interview + 6 months
	Pre-employment vetting	Date of check + 6 months
	Disciplinary proceedings	As specified
	Appraisal	Current year + 5 years
	Allegation of a child protection nature against a member of staff including where the allegation is unfounded5	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found, they are to be kept on the file and a copy provided to the person concerned

Health and Safety	Accident reporting: Adults	Current year + 6 years
	Accident reporting: Children	DOB + 25 years
	Injury at work	Current year + 12 years then review
	Policy	Life of policy + 3 years
	Fire Log Books	Current year + 6 years
	Risk Assessments	Current year + 3 years
	COSHH Data	Current Year + 40 years
	Asbestos Monitoring	Current Year + 40 years
Senior Leadership Team	Minutes of meetings	Date of Meeting + 3 Years
	Reports created for SLT Meetings	Date of Meeting + 3 Years
	Academy Development Plans	Life of plan + 6 Years
	Academy Evaluation Forms	Life of plan + 6 Years
Directors/Governors	Minutes of Meetings	Permanent
	Agendas	Date of Meeting
	Reports presented to meetings	Date of meeting + 6 years
	Parental Complaints	Resolution + 6 years (then review before disposal)
	Admissions data	Date of Admission + 1 year
	Admissions Appeals	Date of hearing + 1 year
General	Prospectus	Current Year + 3 Years
	Newsletters	Current Year + 1 Year
	Visitors Book	Current Year + 6 Years
	OFSTED Reports	25 years
	Employers Liability Insurance	Closure of Academy + 40 years
	Maintenance Records	Current Year + 6 Years
Finance	PAYE & NI Returns	Current Year + 6 Years
	Pension Returns	
	Invoices	
	Remittance Advice	
	Bank Statements	
	Cheque Books	
	Bank Reconciliations	

	Petty Cash Records	
	DFE Returns	
	Direct debits	Current year + 1 year
	Contracts	Until expiry + 6 years
	Budgets	Current year + 3 years
	Budget preparation	Current year + 3 years
	Property Title Deeds	Permanent
	Leases	End of lease + 6 years
	Annual Accounts	Current Year + 6 years
	Letting Information	Current Year + 6 years

Appendix 5: Process for dealing with personal data breaches

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 Data Protection Lead.
- The DPL will investigate the report and determine whether a breach has occurred. To decide, the DPL 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 DPL will contact the DPO and alert the Principal and the Chair of Governors
- The DPL 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 DPL will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPL will work with the DPO on 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 DPL 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 within our network storage system.
- Where the ICO must be notified, the DPL and the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPL 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 DPL
    - 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 DPL 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 DPL expects to have further information. The DPL will submit the remaining information as soon as possible
- The DPL 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 DPL 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 DPL and 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 DPL 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 DPL 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 retained.
- The DPL 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

Appendix 6: Personal Data Breach Record

Date: / /	Person responsible for dealing with breach				
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					
A description of the likely consequences of the personal data breach					
A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects					
Reported by					
Phone/email sent to DPO dposchools@somerset.gov.uk	y/n	Is this high risk?	y/n	Report to ICO	y/n
Date reported to data subjects					
Notes					
Actions approved by		Date	/ /		