CHILDREN FIRST NURSERY AND FOREST SCHOOL

WORTHING COLLEGE

DATA PROTECTION POLICY

OCTOBER 2018

Policy name:	Data Protection Policy
Author:	Kim Frost/Kirsty Cable
Approved by SMT:	Oct 2018
Approved by Corporation:	N/A
Date for next review:	Oct 2020

Through its policies and in its day to day work, the college is committed to promoting equality and fairness and combating discrimination. This applies to everyone, regardless of gender, racial or ethnic background, disability, religion, sexual orientation or age and embraces the college's legal responsibilities.

WORTHING COLLEGE

Mission

To inspire, build confidence and prepare you for the life you want to live.

Vision

"We'll believe in you"

Whatever your background, identity or experience of learning to date, we believe in you. We will support your achievement and success.

"We'll take you further than you expect"

You'll have the opportunity to choose from the widest possible range of courses in one place and we'll stop at nothing to connect you with the best university, employer, or apprenticeship for you. And if you're already working, we'll help you to keep developing and growing.

"We'll provide an inspirational environment for you"

You'll experience a warm welcome from our community. You'll grow in confidence, resilience and be ready for progression to the next step in your life, whether that's further study, the world of work or your own unique adventure.

Values

For us to succeed in our mission and vision, the College has shared community values which help pull us together to act in agreed ways as part of an inspirational community:

We listen intently to the voice of those we serve and show unending commitment to continuous improvement and innovation.

We engage fully with the needs of the local community, employers and universities so we can secure your achievement, success and progression.

We respond quickly, so we're always able to give you the best support, information, advice and guidance, just when you need it.

We celebrate together the successes and diversity of our community.

Worthing College Data Protection Policy

1. Purpose of policy

Our college aims to ensure that all personal data collected about staff, students, parents, governors, visitors, customers 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.

3. The data controller

Our college processes personal data relating to parents, students, staff, governors, visitors, customers 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 Governors

The governing board has overall responsibility for ensuring that our college complies with all relevant data protection obligations. The governors have delegated this responsibility to the Principal and Senior Management Team and will monitor and review the policy and procedures every 2 years, or more frequently as required by external parties such as funding agencies or legal requirements.

4.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy. As outlined in the GDPR Article 39, the DPO's responsibilities include, but are not limited to, the following:

- Educating the college and employees on important compliance requirements
- Training staff involved in data processing
- Conducting audits to ensure compliance and address potential issues proactively
- Maintaining records of all data processing activities conducted by the college, including the purpose of all processing activities, which must be made public on request
- Being the first point of contact for individuals whose data the college processes, informing them about how their data is being used, their rights to have their personal data erased, and what measures the college has put in place to protect their personal information
- Reporting to Governors about all data protection matters.
- Being the first point of contact for individuals whose data the college processes, and for the ICO.

The DPO at Worthing College is Ross Fuhrmann, Assistant Principal for Guidance, who can be contacted at r.fuhrmann@worthing.ac.uk.

4.3 The Principal

The Principal is the lead member of SMT responsible for the implementation and operation of this policy within the college. The Principal acts as the representative of the data controller on a day-to-day basis.

4.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Ensuring that personal information about others is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.
- Ensuring that any information they hold about others is kept securely, particularly any sensitive information which they hold about others. Sensitive information should be kept in a locked filing cabinet or drawer and if it is computerised it should be password protected. Sensitive information should not be stored on a memory stick unless this is absolutely necessary in which case it should be encrypted.
- Checking that any information they provide about themselves to the nursery and College in connection with their employment is accurate and up to date.
- Informing the 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

4.5 Parents/ Carers

Parents/ Carers have responsibilities to provide accurate personal data and contact information in order that the Nursey and college can discharge its duty of care. Parents are responsible for:

- Ensuring that all personal data provided to the Nursery and College about themselves is accurate and up to date.
- Informing the Nursery and College of any changes to information they have provided, eg: change of address.
- Informing the college's Data Protection Officer if, when using the College computer facilities, they process personal data about other people.

5. Data protection principles

The GDPR is based on data protection principles that our nursery and 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 nursery and 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 GDPR and in the Data Protection Act 2018:

- 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 (sensitive data), we will also meet one of the 9 special category conditions for processing which are set out in Article 9 of the GDPR and in the Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

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 college's Disposal of Records schedule – see Appendix 2.

6.3 Privacy notices

The nursery and college will provide privacy notices to anyone whose personal information is being collected, stored, processed or transferred, including students, staff, suppliers, customers and employers. These notices will include the following information:

- What data is being collected, processed and stored
- What the data will be used for;
- How long the data will be stored; and
- The legal basis for using the data
- The categories of organisations and people who will have access to the data (for example ESFA when it comes to student data);
- Information about the college including contact details for the Data Protection Officer;

6.4 E mail communications

The College will require a confidentiality and disclaimer notice to appear at the foot of all e mails at the point of origination including -

"The information contained in this electronic mail message is confidential and is intended for the addressee(s) only. If you are not the intended recipient of this e mail please notify the originator immediately. The unauthorised use, disclosure, copying or alteration of this message is strictly forbidden. Worthing College will not be liable for direct, special, indirect or consequential damages as a result of any virus being passed on, or arising from alteration of the contents of this message by a third party."

7. Sharing personal data

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

- We have a statutory duty or other lawful basis to do so, in which case subjects will be notified in advance through privacy notices.
- We share the children's data with their parents / carers to keep them informed about child's progress and to assist with the children's development
- There is an issue with a child or parent/carer that puts the safety of 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 parents/ carers – 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

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.

Data protection law does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, colleges, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need.

8. Subject access requests and other rights of individuals

8.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the nursery and 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.

8.2 Responding to subject access requests

When responding to requests, we:

- 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

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 student is at risk of abuse, where the disclosure of that information would not be in the student's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the student

If the request is unfounded or excessive, we 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 we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

8.3 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. In cases where the lawful basis on which the subject's data is processed is not consent, the withdrawal of consent may impact on the college's ability to deliver the public service or contract in question.
- 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
- 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.

9. Students in social care

The nursery and college will communicate with the Social Worker or Key Worker of children in care in addition to or instead of with the parents / carers, depending upon the circumstances of the individual child.

10. Photographs and videos

As part of our Nursery activities, we take photographs and record images of individuals.

We will obtain written consent from parents / carers for photographs and videos to be taken of them for communication, marketing and promotional materials. We will clearly explain to the parents/ carers how the photograph and/or video will be used.

Uses may include:

- photographs in staff portfolios for courses, NVQ's etc and understand that this may mean an internal/external tutor/assessor and or verifier will see them
- photographs of their child in other children's learning journals and observations

- photographs of my child to be featured in emails to all parents
- Within nursery on notice boards and in college magazines, brochures, newsletters, etc.
- Outside of nursery by external agencies such as the college photographer, newspapers, campaigns
- Online on our college and nursery website or social media pages (no faces will be shown on social media)

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 child, to ensure they cannot be identified, unless consent for this has been given by the parents/ carer.

11. 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 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
- Providing induction training to new 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

12. 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 take care to ensure that the information remains with them until it is secured in another lockable site such as their home.
- Passwords that are at least 8 characters long containing letters and numbers are used to access college computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- Encryption software is used to protect portable devices and removable media, such as laptops and USB devices, when sensitive data is being transported.
- 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.

- 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

13. 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 we cannot or do not need to rectify or update it.

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

The college's Disposal of Records schedule is provided in Appendix 2.

14. Personal data breaches

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

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

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

- A non-anonymised dataset being published on the college website which shows the exam results of students eligible for the college bursary
- Safeguarding information being made available to an unauthorised person
- The theft of a college laptop containing non-encrypted personal data about students

15. 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 the college's processes make it necessary.

16. 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 our college's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

17. Complaints under this policy

Complaints by staff

Any member of staff who considers that the policy has not been followed in respect of personal data about him/herself should raise the matter with the Data Protection Officer. If the matter is not resolved it may be raised as a formal grievance under the Grievance Policy and Procedure.

Complaints by others (students, parents / carers, customers, employers, etc)

Anyone else who considers that the policy has not been followed in respect of personal data about him/herself should raise a complaint through the college Complaints Policy.

18. Links with other policies

This data protection policy is linked to our:

- Child Protection and Safeguarding Policy
- Communications Policy
- Admissions Policy

- Complaints policy
- IT Security policy
- Privacy policy
- Grievance 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.
- 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 in the Principalship folder of the college computer network.
- 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 in the Principalship folder of the college's computer network.
- The DPO and headteacher 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 2: Worthing College Disposal of Records Schedule

1. Management & Organisation

Ref	Record	Minimum Retention Period
1.1	College Policies	Retain while current. Retain 1 copy of old policy for 2 years after being replaced
1.2	Comments/Complaints	5 years after closing. Review for further retention in the case of contentious disputes

2. Students

Ref	Record	Minimum Retention Period
2.17	Nursery student records	20 years

3. Staff

Ref	Record	Minimum Retention Period
3.1	Staff Personnel Records (including, appointment details, training, staff development etc.)	7 years after leaving employment
3.2	Interview notes and recruitment records	Date of interview + 6 months
3.3	Staff Salary Records	7 years after leaving employment
3.4	Staff Sickness Records (copies of Medical Certs)	Current college year + 6 years
3.9	Staff Performance Review	7 years after leaving

4. Finance

Ref	Record	Minimum Retention Period
4.1	Annual budget and budget deployment	Current financial year + 6 years
4.2	Budget Monitoring	Current financial year + 6 years
4.3	Annual Statement of Accounts (Outturn	Current financial year + 6 years

	Statement)	
4.4	Order Books, Invoices, Bank Records, Cash Books, Till Rolls, Lodgement books etc	Current financial year + 6 years
4.6	Audit Reports	Current financial year + 6 years

5. Health & Safety

Ref	Record	Minimum Retention Period
5.1	Accident Reporting (Adults)	Date of incident + 7 years
5.2	Accident Reporting (Students)	10 years after final year of study
5.3	Risk Assessments – work experience locations/students	10 years
5.4	H & S Reports	15 years

Appendix 3: Good practice in data protection – a guide for staff

1. **Adopt a privacy by default mind-set**
2. **Telephone**

- Carry out identity checks before giving out personal information to someone making an incoming call. Perform similar checks when making outgoing calls.
- Limit the amount of personal information given out over the telephone and follow up with written confirmation if necessary

3. **Passwords**

- Ensure that passwords are hard to guess, involving lower and upper case letters, numbers and symbols. Use a different password for work and personal purposes.
- We will mandate regular password changes every 3 months. Avoid writing passwords down.
- Log off your workstation when leaving to prevent unauthorised access, including in the classroom.

4. **Email**

- When sending an email to multiple recipients (eg: to parents) you must blind copy in their email addresses.
- Be very careful when using email to enter the correct address.
- Prevent virus attacks by taking care when opening emails and attachments or visiting new websites. If you are in any doubt, check with IT team.

5. **Post**

- Be careful to ensure that letters are addressed correctly

6. **Your own devices**

- Do not download or store personal data on your own devices or memory sticks. Accessing personal data through the remote server or a secure cloud-based system like Office 365 is much more secure. Ensure your own devices are password protected.
- If you must use a memory stick or laptop to transport personal data this should be on an encrypted device provided by the college.

7. **Paper-based data**

- Question whether it is necessary for you to print out data.
- Paper-based personal data should be kept under lock and key when not being used.
- Clean desks - desks and offices should be clear of personal data when you are not at your desk.
- Be extremely careful if you need to take paper-based data out of the office or off-site that it is not left unattended.
- Dispose of confidential paper waste securely by shredding.

8. **No parental contact**

- When using telephone, post or email, take care to check that the student has not declined parental contact.

9. **Student Track entries**

- Minimise the recording of sensitive data. Use Confidential Information to record sensitive data which should only be available to staff involved with that student.

10. **Marketing / promotions**

- Do not use contact details to promote opportunities which are not supporting the education and enrichment of students.

11. **Visitors**

- Visitors should be signed in and out of the premises and normally accompanied.

12. **Breaches**

- If you are aware of a data breach you must report it to the college's data protection officer straightaway. Not reporting a breach that has occurred as soon as possible, within 72 hours, is a serious contravention of the GDPR and can result in a substantial fine.

13. **Refer concerns to Data Protection Officer.**

Appendix 4: Worthing College Request Form for Access to Data

Under the General Data Protection Regulations (2018), individuals have the right to make a 'subject access request' to gain access to personal information that the college holds about them. Requests for access to your data should be directed in writing, either by letter or email to the college's Data Protection Officer, Ross Fuhrmann at r.fuhrmann@worthing.ac.uk, tel: 01903 275755. Requests should include:

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

When responding to requests, we:

- 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, unless the request is unfounded or excessive, in which case we may charge a reasonable fee which takes into account administrative costs.
- There are limited circumstances in which we will not disclose certain kinds of information. See the college's data protection policy at www.worthing.ac.uk for further information.

It is not necessary for you to complete this form to access your data but it is provided for your convenience if you would like to use it.

I, _____ wish to have access to:

☐ All the data that the College currently has about me, either as part of an automated system or part of a relevant filing system; or

OR

☐ Data that the College has about me in the following categories:

- ☐ Academic marks or course work details
- ☐ Academic or employment references
- ☐ Disciplinary records
- ☐ Health and medical matters
- ☐ Political, religious or trade union information
- ☐ Any statements of opinion about my abilities or performance
- ☐ Personal details including name, address, date of birth etc.
- ☐ Other information : please list below

Address:	Tel:
	Email:
Signature:	Date: