BIRMINGHAM INDEPENDENT COLLEGE

Data Protection Policy

Next review: 30/01/2027

1. Aims

Our college aims to ensure that all personal data collected about staff, students, parents and carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

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:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

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

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living 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.

TERM	DEFINITION
Data controller	A person or organisation that determines the purposes and the means of processing personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The data controller

Our college processes personal data relating to parents and carers, students, staff, governors, visitors and others, and therefore is a data controller.

The college has paid its data protection fee to the ICO, as legally required.

5. 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.

5.1 Governing board

The governing board has overall responsibility for ensuring that our college complies with all relevant data protection obligations.

5.2 Data protection officer (DPO)

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 proprietorship and, where relevant, report to the board their advice and recommendations on college data protection issues.

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

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

Our DPO is Vivienne Lambert and is contactable via vlambert@bicollege.org

5.3 Head of College

The head of college acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing 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 UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals

- If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The UK GDPR is based on data protection principles that our 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.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- 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 or another person i.e. 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 or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the college (where the processing is not for any tasks the college performs as a public authority) 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 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a student) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law

- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a student) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.2 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.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a student 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 students – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor 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

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

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 internationally, we will do so in accordance with UK data protection law. Appendix 1 provides more insight on who we may share your data with.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

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

9.2 Children and subject access requests

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

Secondary colleges add:

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.

9.3 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 (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when 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 (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

10. Parental requests to see the educational record

Academies, including free colleges, and independent colleges: there is no automatic parental right of access to the educational record in our setting.

11. CCTV

We use CCTV in various locations around the college site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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.

Any enquiries about the CCTV system should be directed to Ms Lambert, Operations Manager.

12. Photographs and videos

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

Where the college takes photographs and videos, uses may include:

- Within college on notice boards and 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. A sample permission form can be seen in appendix 2 below.

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.

13. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Birmingham Independent College recognises that AI has many uses to help students learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Birmingham Independent College will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

14. 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 data protection 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
- 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

15. 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, 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 10 characters long containing letters and numbers are used to access college computers, laptops and other electronic devices. Staff and students are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, students or proprietors 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 (see section 8)

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

17. 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 3.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. 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 student premium
- Safeguarding information being made available to an unauthorised person
- The theft of a college laptop containing non-encrypted personal data about students

18. Training

All staff and proprietors 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.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the proprietorship.

Appendix 1: Who we Share data with and why

Career Guidance

As part of our statutory obligation to provide impartial careers advice and guidance we will work with the WSCC Careers Adviser and pass names of students needing additional information, advice or guidance at transitional points on to them. We will also work with TheCareers Enterprise Company through their Enterprise Advisory Network [provided by Coast toCapital, LEP] and the National Collaboration Outreach Project [NCOP]and provide statistical data about students to aid the allocation of funding and resources. The school will also provide its independent careers adviser with student names and age for the purpose of 1-1 guidance interviews delivered on site.

Exam Boards

Students' exams-related data may be shared with the following organisations:

- Awarding bodies
- Joint Council for Qualifications
- Department for Education; Local Authority;

This data may relate to exam entries, access arrangements, the conduct of exams and non-examination assessments, special consideration requests and exam results/post- results/certificate information.

Department for Education (DfE).

We are required to share information about our pupils with our local authority (LA) and theDepartment for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013. To find out more about the data collection requirements placed on us by the Department for Education go

to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Some of this information is then stored in the National Pupil Database (NPD). The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.To find out more about the NPD, go

to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information

The DfE may also share pupil level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with GDPR

Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to pupil level data,requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

For more information on how this sharing process works, please

visit: https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract

For information on which third party organizations (and for which project) pupil level datahas been provided to, please visit:

https://www.gov.uk/government/publications/national-pupil-database-requests-received

If you need more information about how the local authority and/or DfE collect and use yourinformation, please visit:

- our local authority at www.birmingham.gov.uk
- or the DfE website at https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Clinical Commissioning Groups (CCGs)

We are required, by law, to pass certain information about our pupils to CCGs.

CCGs use information about pupils for research and statistical purposes, to develop, monitorand evaluate the performance of local health services. These statistics will not identify individual pupils. It is necessary for certain health information about children (for example, such as their height and weight) to be retained for a certain period of time (designated by the Department of Health) and requires these CCGs to maintain children's names and addresses for this purpose. CCGs may also provide individual schools and Local Authorities (LAs) with aggregated health information which will not identify individual children.

Local Authority - education and training

We are required, by law, to pass certain information about our pupils to local authorities.

The LA holds information about young people living in its area, including about their education and training history. This is to support the provision of their education up to theage of 20 (and beyond this age for those with a special education need or disability).

Education institutions and other public bodies (including the Department for Education (DfE),police, probation and health services) may pass information to the LA to help them to do this.

The LA shares some of the information it collects with the Department for Education (DfE) toenable them to; produce statistics, assess performance, determine the destinations of youngpeople after they have left school or college and to evaluate Government funded programmes.

The LA may also share information with post-16 education and training providers to secureappropriate support for them. They may also share data with education establishments which shows what their pupils go on to do after the age of 16.

For children under 16, a parent or guardian can ask that no information other than their child's name, address and date of birth (or their own name and address) be passed to a localauthority. This right transfers to the child on their 16th birthday. Pupils and/or a parent/guardian will need to inform the school/LA if this is what they wish. If you want to see a copy of information about you that the LA holds, please contact:

The Data Protection Officer
Birmingham City Council Victoria
Square Birmingham

B1 1BB

Local Authority – social services

In order to comply with our statutory safeguarding duties we are required, by law, to passcertain information about our pupils to local authorities. Information will only be shared where it is fair and lawful to do so.

If you want to see a copy of information about you that the LA holds, please contact:The Data Protection Officer
Birmingham City Council
Victoria Square Birmingham
B1 1BB

Police, Fire and Rescue Service, Ambulance Service and other emergency or enforcement agencies

In order to comply with our duty of care to pupils, our statutory safeguarding duties and ourobligations in respect of the prevention and detection of crime, we may also share personal data with other statutory and partnership agencies.

Appendix 2: BIC Permission Form

Student's Name:

Accreditation evidence

In order to show achievements and progress of our students, it is the school policy to gather some evidence using photographs and/or video. Without this some students would be unlikely to gain qualifications. This information remains in college in the care of administration and staff.

If you are concerned about this in any way, please write to Ms. Lambert or contact the college by email on info@bicollege.org

On the form below please indicate your level of permission for use of photographs/videos of your child. We will only use photographs/video at other levels if you give consent.

Photographs/videos for use in college only

This includes for example photographs/video of students on display in classrooms.

I give my consent	
I do not give my consent	

Photographs/video that we will publish to our website, prospectus or elsewhere.

We will NOT name students if you give this level of permission.

I give my consent	
I do not give my consent	

Photographs/video accompanied by your child's first name only and published on our website, prospectus or elsewhere.

I give my consent	
I do not give my consent	

Additional consent required for photos used for school purposes

Sometimes your child will have a photo taken of them working with other students in their class or may even be in the background of another student's photo. Therefore, some photos that we share with other families may have your son/daughter in them or in the background of them.

I hereby give consent for such images to be shared.

I give my consent	
I do not give my consent	

Educational Visits

During the course of the school year your child will be going out on education visits to various locations in the Birmingham area, these visits will NOT include any hazardous activity.

I give my consent	
I do not give my consent	

Trampoline Permission

We have a trampoline in our complex needs classroom on the ground floor. Students will have the opportunity to use this equipment, one at a time, and accompanied by staff at all times.

We will assess them to check they are able to use it safely on their first use.

I give my consent	
I do not give my consent	

My child is familiar with trampolines, has used one regularly, and safely before, please select Yes or No.

Yes	No

Massage Permission

There may be times when we practice hand and foot massage with our students.

I give my consent for HAND massage	
I do not give my consent for HAND massage	

I give my consent for FOOT massage	
I do not give my consent for FOOT massage	

Community Access Permission

Community access and preparing for adulthood form an important part of our curriculum and so we ask for general consent for your child to go out on local visits during the course of the academic year, and we will inform you of regular local area visits at the beginning of each term via letter /email home. We will inform you separately and ask for additional consent for any visits beyond the local area.

I give my consent	
I do not give my consent	

Healthy snacks permission

Occasionally, students can be provided with snacks or food that has been cooked during cookery or life skills lessons. Students dietary requirements will be kept at all times.

I give my consent to food made during lessons	
I do not give my consent to food made during lessons	

I am aware that I may withdraw my consent at any time by notifying the college.

If at any point you are concerned about anything you see on the website, please let us know immediately and we will to happy to remove or amend it according to your wishes.

Your Signature:	Date:

Appendix 3: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach or potential breach, the staff member, proprietor or data processor must immediately notify the data protection officer (DPO) by email at vlambert@bicollege.org.
- 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
- Staff and proprietors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the head of college and the chair of proprietors.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the college's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the college's awareness of the breach. 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 of the college's awareness of the breach. 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
- Where the college is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - 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 consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored, on the college's computer system,
- The DPO and head of college will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the college to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the external IT support provider to attempt to recall it from external recipients and remove it from the college's email system (retaining a copy if a required as evidence).
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the college should inform any, or all, of its local safeguarding partners.

Other types of breach that you might want to consider could include:

- Details of student premium interventions for named children being published on the college website
- Non-anonymised student exam results or staff pay information being shared with governors
- A college laptop containing non-encrypted sensitive personal data being stolen or hacked
- The college's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong students or families