Data Protection

Policy and Procedure

Document Status	Live & Current
Document Type	Policy POL010
Version	1
Issue	3
Document Date	January 2021
Review Date	January 2022
Reviewer	Thomas Nolan
Publication	Controlled Hard Copy and Google Drive

1. Aims and Scope

Barfection Limited works to ensure that all personal data about staff, students, visitors and stakeholders is collected, stored and processed as per the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) requirements.

This policy applies to:

- All staff and volunteers of Barfection Limited
- All contractors, suppliers and other people working on behalf of Barfection Limited
- All personal data, regardless of whether it is in paper or electronic format

2. Legislation and Guidance

This policy is based upon requirements of the GDPR and DPA 2018 and utilises guidance published by the Information Commissioner's Office (ICO).

3. Definitions

Term	Definition
Personal data	Any information relating to an identified or identifiable individual. For example, • 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 • Religions or philosophical beliefs • Trade union membership • Genetics • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

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

4. The data controller

Barfection Limited processes personal data relating to staff, students, visitors, stakeholders and others, and therefore is a data controller.

5. Roles and responsibilities

Board of Directors

The Board of Directors has overall responsibility for ensuring that the organisation complies with all relevant data protection obligations.

Data protection officer

Barfection Limited does not currently need to appoint a Data Protection Officer

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing Barfection Limited of any changes to their personal data, such as a change of address
- Contacting the Directors 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 EU area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that the organisation 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

7. Collecting personal data

Lawfulness, fairness and transparency

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

- The data needs to be processed so that Barfection Limited can fulfil a contract with the individual, or the individual has asked the organisation to take specific steps before entering into a contract
- The data needs to be processed so that the organisation 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 for the legitimate interests of the organisation or a third party (provided the individual's rights and freedoms are not overridden)
- The individual has freely given clear consent

For special categories of personal data, there must also be present one of the special category conditions for processing which are set out in the GDPR and DP 2018.

Whenever personal data is first collected from an individual, relevant information will be provided as required by data protection law.

Limitation, minimisation and accuracy

Personal data will only be collected for specified, explicit and legitimate reason. These reasons will be explained to the individuals when the data is first collected.

If the personal data is required to be used for a reason other than those given when first obtained, the individuals concerned will be informed before any actions and consent sought where necessary.

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

When staff no longer require the personal data they hold, it must be deleted or anonymised as per DP 2018.

8. Sharing personal data

Personal data will not normally be shared with anyone else, unless:

- There is an issue with a student that puts the safety of our staff at risk
- There is a need to liaise with other agencies – although consent will be sought as necessary before doing this
- Suppliers or stakeholders need data to enable Barfection Limited to provide services to staff and students. For example, work placements or IT companies. When doing this:
    - Only suppliers or stakeholders who can provide sufficient guarantees that they comply with the data protection law will be used
    - A data sharing agreement with suppliers or stakeholders will be established, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data shared
    - Only data that is needed to carry out a service or to keep them safe will be shared with suppliers or stakeholders

Personal data will also be shared with law enforcement and government bodies where legally required, 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 safeguarding obligations
- Research and statistical purposes, ensuring personal data is sufficiently anonymised or consent is provided

Personal data may also be shared with emergency services and local authorities to assist with emergency situations that affect students or staff.

9. Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the organisation 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 is not 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 or email to the directors. The 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 directors.

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, subject access requests to Barfection Limited for students aged under 18 from parents or carers may not be granted without the express permission of the student. However, the student's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, Barfection Limited:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge
- May tell the individual that their request will be fulfilled within three months of receipt, where a request is complex or numerous. The individual will be informed of this within one month and given an explanation of the extension as necessary

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 disclose of that information would not be in the student's best interest
- Is contained in adoption or other parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, Barfection Limited 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 a request is refused, the individual will be told why and given details of how to complain to the ICO.

Other data protection rights of the individual

In addition to the right to make a subject access request and to receive information when data is being collected, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask Barfection Limited 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 directors. If staff receive such a request, they must immediately forward it to the directors.

10. CCTV

CCTV is used in some locations to ensure it remains safe. Barfection Limited will adhere to the ICO's code of practice for the use of CCTV.

Individuals' permission is not required to use CCTV, but it is clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the Directors.

11. Photographs and videos

As part of learning activities, photographs and recorded images of individuals may be taken.

Written consent from parents/carers or students aged 18 and over will be obtained for photographs and videos to be taken for communication, marketing and promotional materials.

Where parental consent is required, a clear explanation of how the photograph and/or video will be used will be given to both the parent/carer and student. Where parental consent is not required, a clear explanation of how the photograph and/or video will be used will be given to the student.

Uses may include:

- Within the organisation's notice boards, magazines, brochures, newsletters, prospectus etc.
- Outside of Barfection Limited by external agencies such as the external photographer, newspapers, campaigns
- Online on the company website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, the photograph or video will be deleted and not distributed any further.

When using photographs and videos in this way personal information about the individual will not be included to ensure they cannot be identified.

12. Data protection by design and default

Measures will be put in place to show that data protection is integrated into all data processing activities, including:

- Appointing a suitably qualified person, 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
- Completing privacy impact assessments where the organisation's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the directors 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
- Regularly conducting reviews and audits to test privacy measures and ensure compliance
- Maintaining records of processing activities, including:

- For the benefit of data subjects, making available the name and contact details of the organisation and directors and all information required to share about how personal data is used and processed
- For all personal data held, maintaining an internal record of the type of data, data subject, how and why the data is being used, any third-party recipients, how and why the data is being stored, retention periods and how the data is being kept secure

13. Data security and storage of records

Personal data will be protected and kept 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 or classroom desks, 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 ensure that this is necessary information and return it as a priority
- Passwords that are at least 8 characters long containing letters and numbers are used to access company computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- Where personal data is needed to be shared with a third party, due diligence is carried out and reasonable steps to ensure it is stored securely and adequately protected are taken

14. 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 it cannot be or does not need to be rectified or updated.

For example, paper-based records will be shredded or incinerated, and electronic files overwritten or deleted. If a third party is used to dispose of records, a sufficient guarantee regarding compliance with data protection law will be sought.

15. Personal data breaches

Barfection Limited will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, the procedures set out in appendix 1 will be followed.

When appropriate, the data breach will be reported to the ICO within 72 hours. Such breaches may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a company laptop containing non-encrypted personal data about students
- Personal data being posted on social media or online without consent or anonymising

16. Training

All staff and directors 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 company's processes make it necessary.

17. Monitoring arrangements

The directors are responsible for monitoring and reviewing this policy. This policy will be reviewed and updated if necessary due to a legislative change, change in process or annually.

18. Retention periods for different categories of data

Type of data	**When will the College delete it?**	**Action following Retention**
Accidents and Insurance		
Accident reports and relevant correspondence	3 years after settlement Insurance schedules	Destroy
Insurance Claims correspondence	80 years	Destroy
Contracting and Tenders		
Income Contracts - Contractual documentation including original contract and any contract variations, notices / correspondence, performance and notes of meetings	Termination of contract / financial year in which contract terminated + 6 years (unless a Deed and then + 10 years, or ESF cofinanced - 2007/13 until at least 31 December 2022 or 2014/20 until at least 31 December 2030)	Destroy
Expenditure Contracts - Contractual documentation including original contract and any contract variations, notices / correspondence, supplier performance and notes of meetings	Termination of contract / financial year in which contract terminated + 6 years (unless a Deed and then + 10 years, or ESF cofinanced - 2007/13 until at least 31 December 2022 or 2014/20 until at least 31 December 2030)	Destroy
Service Level Agreements (non-monetary) - Original SLA and any contract variations, notices / correspondence, performance and notes of meetings	Termination of contract / financial year in which contract terminated + 6 years (unless a Deed and then + 10 years, or ESF cofinanced - 2007/13 until at least 31 December 2022 or 2014/20 until at least 31 December 2030)	Destroy
Agents Contracts - Contractual documentation including original contract and any contract variations,	Termination of contract / financial year in which contract terminated + 6 years (unless a Deed and then + 10 years, or ESF cofinanced - 2007/13 until at least 31	Destroy

notices / correspondence, supplier performance and notes of meetings	December 2022 or 2014/20 until at least 31 December 2030)	
Indemnities and guarantees	6 years after expiry or longer as determined by the Contract	Destroy
Disputes and Litigation - Records documenting negotiation, establishment and settlement of dispute and / or claims	Settlement of claims + 6 years OR withdrawal of claim + 6 years	Destroy
Records as defined by the Contract - Documents required to be held in accordance with income, expenditure, agent contracts or SLAs, e.g. learner records	Termination of contract / financial year in which contract terminated + 6 years (unless a Deed and then + 10 years, or ESF cofinanced - 2007/13 until at least 31 December 2022 or 2014/20 until at least 31 December 2030)	Destroy
Intellectual Property - any copyright, patent and trade mark records	Permanently	Destroy
Tender documents	7/15 years	Destroy
Corporate Governance		
Policies and Procedures - Records documenting the development and establishment of policies and procedures	Superseded + 5 years	Destroy
Statutory Records and Registers - memorandum and articles of association - certificate of incorporation - seal book/register - register of directors and secretaries, directors' interests, interests in voting shares, charges and members - Minutes of general and class meetings, directors' minutes, written resolutions	Originals to be kept permanently	Destroy
Estates		
Agreements with architects builders etc	Six years after contract completion	Destroy
Deeds of Title	Permanently	Destroy
Leases	Twelve years after lease has terminated	Destroy
Licensing agreements	Six years after expiry	Destroy
CCTV recordings	28 days	Destroy
Security Information	Current academic year + 5 years	Destroy

Examinations		
Records documenting & establishment of College's assessment & examination including the control of examination papers & scripts and timetabling of examinations	10 years	Destroy
Records documenting the organisation of examination facilities, including special arrangements for learners with special needs	2 years	Destroy
Arrangements for assessment & examinations	7 years	Destroy
Pass/Qualification/Award Lists	10 years	Destroy
Finance and Accounting		
Financial Forecasts	3 years	Destroy
Capital and Revenue Budgets	3 years	Destroy
European Funding - All original documentation including: - Application Form and approval letters - Claim forms - Audit Reports - Project closure report - Match Funding Certificates - All correspondence - Project records - Individual beneficiary records - Financial records	For a period of 6 years following final payment by the European Commission to DWP	Destroy
Accounting for income	6 years	Destroy
Sales ledgers, credit notes, till rolls, remittance advices	6 years	Destroy
Sales invoices	6 years	Destroy
Statements	1 year	Destroy
Accounting for expenditure	6 years	Destroy
Payment authorisations, credit notes, purchase ledgers, cheque authorisations, BACS reports, staff expense claims, petty cash authorisations, petty cash receipts, petty cash books, journal vouchers	6 years	Destroy
Purchase invoices	6 years	Destroy

Financial analysis	Permanent	Destroy
Annual Financial Statements	Permanent	Destroy
Monthly Management Accounts	1 year	Destroy
Bank accounts	6 years	Destroy
Pay-in slips	6 years	Destroy
Cash receipt data	6 years	Destroy
Bank Statements	6 years	Destroy
Cancelled cheques	6 years	Destroy
Capital Asset Register - major items	Permanent	Destroy
Capital Asset Register - other items	12 years	Destroy
Asset Disposal Authorisation Forms	1 year	Destroy
Journal accounting transactions	1 year	Destroy
Monitoring of actual against planned expenditure	1 year	Destroy
Budget reports	1 year	Destroy
Acquisition/disposal of investments	Permanent/ 6 years after disposal	Destroy
Investment instructions	6 years	Destroy
Share Certificates	6 years	Destroy
Investment Portfolio Reports	6 Years	Destroy
Assessment of tax liabilities	6 years	Destroy
VAT account	6 years	Destroy
Submission of Tax Returns	6 years	Destroy
VAT Return	6 years	Destroy
Corporation Tax Returns	2 years	Destroy
PAYE/NI/Returns	6 years	Destroy
Register of Gifts & Hospitality received	6 years	Destroy
Funding		
Compare ILR records (data dumps)	Current academic year + 7 years	Destroy
External Funding Submission reports	Current academic year + 7 years	Destroy
ILR Funding Software outputs (MDB format)	Current academic year + 7 years	Destroy
ILR raw data files (XML or Flat File formats)	Current academic year + 7 years	Destroy

Planning tools	Current academic year + 7 years	Destroy
Records relating to Planning and performance monitoring meetings.	Current academic year + 7 years	Destroy
Records relating to the Annual Assurance Plan	Current academic year + 7 years	Destroy
Records relating to the carrying out and reporting of external audits	Current academic year + 7 years	Destroy
Records relating to the carrying out and reporting of internal audits	Current academic year + 7 years	Destroy
Exec reports	Current academic year + 7 years	Destroy
Health and Safety		
Accident records/reports (see below for accidents with potential to cause ill health under COSHH or Asbestos) (H&S)	6 Years	Archive
Asbestos	Permanent	Archive
Emergency Procedures	3 Years	Archive
Fire appliances	Fire alarm and detection system test & maintenance records 3 years, Fire evacuation drills	Archive
Fire Risk assessment	Permanent	Archive
H&S Audits and Inspections	Permanent - 6 years archive	Archive
Health and Safety Policy	Permanent - 6 years archive	Archive
H&S Training Records: all types of training	6 years	Destroy
Health and Safety Meetings, Plans, Safety Committees and Groups (H&S)	6 Years	Destroy
Medical records containing details of employees exposed to asbestos, noise medical examination certificates (HR)	40 years	Archive
Medical/Health Surveillance records as specified by the Control of Substances Hazardous to Health Regulations (COSHH) (HR)	40 years	Archive
RIDDOR Reports	10 years	Destroy
Risk Assessments (H&S)	10 Years	Destroy
Statutory testing and inspection work equipment, systems records,	3, 5 10 years depending upon premises plant and equipment	Archive

Stop Notices and other Court Orders	Originals to be kept permanently	Archive
Water Hygiene management	10 Years	Destroy
Marketing		
Promotional Material	Current Academic Year + 3	Archive
Press Cuttings	Current Academic Year + 1	Archive
Public Relations	Current Academic Year + 1	Archive
Prospectuses	Current Academic Year + 1	Archive
Quality and Standards		
Inspection Documents	10 Years	Archive
Complaints Procedure and records of complaints	5 years	Destroy
Records documenting the development of training and development programmes to meet defined needs in relation to Observation of Learning and Assessment and Data and Information.	Completion of programme + 5 years	Destroy
Records containing individual feedback on training and development programmes in relation to Observation of Learning and Assessment.	Completion of analysis of feedback	Destroy
Records documenting the conduct and results of formal internal reviews of teaching quality, and responses to the results.	Current academic year + 5 years	Destroy
Records documenting the conduct and results of external reviews and audits of teaching quality and standards.	Next Review completed + 5 years	Destroy
Records documenting the conduct and results of formal reviews of the institution's programmes and courses and responses to the results.	Current academic year + 10 years	Destroy
Records documenting the process of obtaining approval and/or accreditation for taught programmes from professional, statutory or other accreditation bodies.	Life of programme	Destroy

Records containing reports of routine internal reviews of taught courses in relation to Observation of Learning and Assessment and performance	Current academic year + 5 years	Destroy
Records documenting the conduct and results of formal reviews of taught courses in relation to Observation of Learning and Assessment and Quality, and the responses to the results.	Current academic year + 5 years	Destroy
Staffing		
Expense accounts- Purchase invoices	Scanned – disposed of after 6 months	Destroy
Health insurance records	12 years after final cessation of benefit	Destroy
Holiday records	7 years after employment ceases	Destroy
Payroll records	6 tax years plus the current tax year	Destroy
Pension Records	30 years after employment ceases	Destroy
Recruitment records	6 months	Destroy
Employee files and training records (including disciplinary records and working time records)	7 years after employment ceases	Destroy
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	7 years from the date of redundancy	Destroy
Statutory Sick Pay records, calculations, certificates, self-certificates	6 tax years plus the current tax year	Destroy
Trade Union agreements	10 years after ceasing to be effective	Destroy
References	7 years after employment ceases	Destroy
Occupational Health Records	7 years after employment ceases	Destroy
Employment Tribunal Requests	7 years after employment ceases	Destroy
Declaration of Outside Employment	7 years after employment ceases	Destroy
Performance Review & Development Information	7 years after employment ceases	Destroy
Students		

Records documenting the handling of enquires from prospective students	Current academic year + 1 year	Destroy
Records containing summaries and analyses of enquiry, recruitment and retention data	Current academic year + 1 years	Destroy
Records documenting the handling of applications: successful applications	End of student relationship + 1 years	Destroy
Records documenting the handling of applications for admission: unsuccessful applications	Current academic year + 1 year	Destroy
Records documenting the enrolment of individual students on courses	Termination of relationship + 6 years (unless ESF co-financed - 2007/13 until at least 31 December 2022 or 2014/20 until at least 31 December 2030)	Destroy
Records containing personal data on individual students	Termination of relationship + 6 years (unless ESF co-financed - 2007/13 until at least 31 December 2022 or 2014/20 until at least 31 December 2030)	Destroy
Records containing standard analyses of data from individual students' records. Records documenting the handling of requests for confirmation of individual students' awards, attendance or conduct from employers and other educational institutions	Current academic year + 6 years	Destroy
Records documenting the progress of individual students and formal action taken by the institution to deal with unsatisfactory progress	Termination of relationship + 6 years (unless ESF co-financed - 2007/13 until at least 31 December 2022 or 2014/20 until at least 31 December 2030)	Destroy
Records documenting the conduct and results of disciplinary proceedings against individual students	Last action on case + 6 years	Destroy
Coursework (including projects & reports)	Termination of relationship + 3 years	Destroy
Examination certificates	Current academic year + 1 year	Destroy
Records documenting the attendance of individual students on courses	Termination of relationship + 6 years (unless ESF co-financed - 2007/13 until at least 31 December 2022 or 2014/20 until at least 31 December 2030)	Destroy
Individual Learning Plans	Termination of relationship + 6 years (unless ESF co-financed - 2007/13 until at	Destroy

	least 31 December 2022 or 2014/20 until at least 31 December 2030)	
Vehicles		
Rental and hire purchase agreements - Vehicles only	6 years after expiry	Destroy
Vehicle registration records, MOT, Certificates and vehicle maintenance records	2 years after disposal of vehicle	Destroy

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 directors
- The directors will investigate the report and determine whether a breach has occurred. To decide, the directors 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 directors 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 directors will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The directors 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 directors 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 directors must notify the ICO.

- The directors will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's server.
- Where the ICO must be notified, the directors will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the directors 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 directors
    - 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 directors 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 directors expect to have further information. The directors will submit the remaining information as soon as possible
- The directors 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 directors 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 directors
    - 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 directors 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 directors 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 company server

- The directors will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

The actions set out below will be taken to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. The effectiveness of these actions will be reviewed and amended 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 directors as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the directors will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the directors will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request

that those individuals delete the information and do not share, publish, save or replicate it in any way

- The directors will ensure a written response from all the individuals who received the data is received, confirming that they have complied with this request
- The directors will carry out an internet search to check that the information has not been made public; if it has, the publisher/website owner or administrator will be contacted to request that the information is removed from their website and deleted

Other types of breach for consideration include:

- Non-anonymised student exam results being shared with unauthorised people
- Staff pay information being shared with unauthorised people
- A company laptop containing non-encrypted sensitive personal data being stolen or hacked.

Appendix 2 : Subject Access Request Form

Date:

To: Barfection Limited

Re: subject access request

Dear Company Directors,

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me and verify the lawfulness of the processing.

Here is the necessary information:

Name	
(Relationship with Barfection Limited)	Please select: Learner/parent/employee/stakeholder/volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example: • Your personnel file • Yours or your child's behaviour record

If you need any more information from me, please let me know as soon as possible.

Please bear in mind that under the GDPR you cannot charge a free to provide this information, and in most cases, must supply me with the information within 1 month.

If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at www.ico.org.uk

Yours sincerely,