Bay Learning Academy CIC

Data Protection and Communication Policy 2024 - 2025

in accordance with

UK General Data Protection Regulation (UKGDPR)

Data Protection Policy (UK General Data Protection Regulation)

Statement of Policy

- Bay Learning Academy needs to collect and use certain types of information about learners, their families, employees and with whom it deals, in order to perform its functions. This includes information on current, past and prospective employees, learners, persons with parental responsibility, suppliers, customers, service users and others with whom it communicates. Bay Learning Academy is required by law to collect and use certain types of information to fulfil its statutory duties and to comply with the legal requirements.

- The Principal is responsible for data and ensuring the academy is GDPR compliant. Any breaches should be reported to the Principal in the first instance as Data Controller.

- This policy should be read in conjunction with 'Children and the UKGDPR' at https://ico.org.uk

1. Policy Aims

- This policy outlines the Academy's arrangements to access personal information by learners, persons with parental responsibility, public and employees in accordance with the UK General Data Protection Regulation (UKGDPR) and the Data protection Act 2018 and PECR Privacy and Electronic Communication Regulation.

- This policy will be communicated to all employees and is accompanied by notes of guidance. This policy will be published to employees through the academy's website.

- The policy applies to all personal information held by the Academy irrespective of ownership. Personal information is defined for the purposes of this policy as being any information from which an individual can be identified (including Computer storage, Documents, Photographs, CCTV images, Voice, etc.).

- The policy applies to information held by the academy, irrespective of ownership, which can identify an organisation and the communication of this information.

1. Scope

- The policy also applies to all contractors and agencies operating on behalf of the Academy on the Goodwin Development Trust premises. For the purpose of this policy, the term 'employee' covers all of these groups.

2. Policy Objectives

- This policy outlines the Academy's approach to ensuring all employees effectively process and manage personal information within set standards, to protect the privacy of individuals and organisations, to comply with the principles and requirements of the UKGDPR and other relevant legislation. All employees complete training on procedures that comply with UKGDPR, when handling personal information about Learners, Parents, Visitors, Clients, Contractors and Employees.

- This policy should be complied with for personal information relating to all individuals whether deceased or living.

- The policy and guidelines cover requests for information from individuals for their own personal data. Such requests, defined as subject access requests (SAR's), should be handled in accordance with this policy, in compliance with UKGDPR.

- A definition of terms is available at Appendix A.

- To promote the effective, consistent and legal processing of personal information by defining a personal information handling policy.

- To ensure that all employees are aware of their responsibilities in relation to the processing of personal information and to the law surrounding its use.

- To ensure that all employees are aware of the consequences of the misuse or abuse of personal information.

- To establish and maintain trust and confidence in the Academy's ability to process personal information.

- To ensure compliance with post Brexit legislation, guidance and standards relating to the handling of personal information.

3. Monitoring & Review

- The policy and guidelines will be reviewed when necessary to take into account changes in legislation and to ensure that they remain timely and relevant. Any changes will be publicised through the Information Commissioners Office (ICO) and normal communication channels.
- The effectiveness of the policy will also be assessed through the monitoring of requests for personal

information, the Academy's responses to these, and complaints. These events will be collated into an annual report. Where issues of concern arise, then the Information and Security Officer (ISO) will be approached.

- The policy will be published on the Academy's website and hard copies will be provided upon request.

- An information audit will be conducted every three years by the Academy and any recommendations complied with, within agreed timescales. This also complies with Section 46 of the Freedom of Information Act.

4. Procedure

- The Academy regards the lawful and correct treatment of information as critical to successful operations and to maintaining confidence between those with whom it deals. It is essential that it treat information lawfully and correctly and with express permission from the Principal.

- The purpose of the UKGDPR is to protect the rights and privacy of living individuals. It regulates the processing of personal information including the obtaining, holding, use or disclosure of such information. It places obligations on those who record and use personal information and gives rights to those whose information is being processed.

5. Processing Information

- The processing of information is defined as encompassing everything that we do with information including the sharing, transferring or disclosing of information to another organisation or internally. This includes the use of social media. Information can only be shared, transferred or disclosed with the express permission of the Principal or where this information disclosure is in accordance with the law see 7.11 for examples.

- Personal information must be processed in accordance with the six principles under the UKGDPR unless an exemption applies.

- Employees must respect information that they have access to and treat it in the manner in which they would expect their personal details to be treated.

- Employees must have regard and respect for the privacy of learners, persons with parental responsibility and employees and process their information accordingly.
- Access to information must be accepted by all, to be on a need and a right to know basis.

- Personal Information should be deleted and disposed of under principles of UKGDPR.

- Personal information will be held securely and be accessible only by those with a need and a right to know. The Principal is responsible for ensuring that personal information held at the academy is surrounded by appropriate security, i.e. relevant to the sensitivity of the personal information being

processed.

- Arrangements and contingencies need to be in place in order to protect personal information from loss due to natural and unnatural disaster, e.g. flood, arson, theft.

- Personal information must not be transmitted or transported externally via manual or electronic means without appropriate security. Portable devices (laptops, CDs, DVD's, USB memory sticks, etc.) which contain personal information must use adequate security measures e.g. encryption, to protect against losses or access by unauthorised persons. The Data Controller/ Principal requests that no identifiable collected information will be accessed by laptops unless encrypted. This is because collected data is the responsibility of the Data Controller / Principal (see ref. encryption at www.ico.org.uk)

- Personal information must be disposed of safely and securely when it has reached the end of its shelf life.

- Information will not be passed on to any third party unless any one or more of the following apply (Principles of UKGDPR):

- Explicit consent from both the Principal and the Data subject is obtained
- The organisation requesting the information has a legal right to the information (e.g. police investigating crime)
- It is a requirement of law
- It is to comply with a court order
- It is necessary to provide educational services
- The Academy believes it is in the subject's own interest
- The Academy believes it is in the overall public interest and in a particular instance this is judged to outweigh the other considerations
- At the point of collection and disclosure, the data subject will be informed of the purposes for which the information is being collected, processed or disclosed together with any other relevant details. At this time, where choices are available, the child/young person or persons with parental responsibility or organisation will be given the opportunity to opt out of the information processing arrangements.

- The Academy will promote good practice in the sharing of information with its partners, government agencies and departments and other public and private sector organisations. All sharing will comply with the UKGDPR and the current General Information Sharing Protocol (GISP).

- The quality and accuracy of personal information should be relevant to the purpose for which it is to be used.

- The purposes for which personal information is processed in the Academy will be detailed in the academy Data Protection Notification, which will be renewed annually with the Information Commissioners Office.
- Any changes to purposes must be identified to the Information and Security Officer (ISO) who will submit amendments as required.

- Processing of information for a purpose not reflected in the UKGDPR or in the notification must be approved by the ISO.

- Any inaccurate or misleading information will be checked and corrected as soon as the school, learner, parent or organisation brings this to the Academy's attention.

- The rights of data subjects as defined by the UKGDPR 2016, and specifically their right of access to their own personal information will be complied with fully and given appropriate respect and priority.

6. Data Security and Storage of Records

- Personal information must be stored securely, accessible only to those with a legitimate need.
- The Principal ensures personal information is protected by appropriate security measures proportionate to the sensitivity of the data.
- Digital records must be protected by strong passwords, encryption, and access control.
- Physical records must be stored in locked cabinets or secure storage rooms.
- Measures must be in place to protect data against loss from natural disasters, cyber-attacks, or theft.
- Any portable devices containing personal information (e.g., USBs, laptops) must use encryption and password protection.

7. Disposal of Records

- Personal information must be securely deleted or shredded when it is no longer needed.
- Digital records must be permanently deleted from storage and backup systems.
- Records containing sensitive or special category data must be disposed of via approved destruction methods.
- Data must not be deleted or disposed of after a Subject Access Request (SAR) unless requested by the subject.
- Employees must follow the Academy's Data Retention Policy, ensuring data is only retained for the legally required period.
- Personal Data Breach Procedure
- A data breach occurs when personal information is lost, disclosed, or accessed without authorization. If a data breach occurs:
- Identify and Contain the Breach
- The individual discovering the breach must report it immediately to the Principal (Data Controller).
- The Principal must assess the severity and determine containment actions.
- Risk Assessment
- Evaluate the nature of the data involved (e.g., special category data, financial details, personal identifiers).
- Assess the potential harm to affected individuals (e.g., identity theft, financial loss, distress).
- Report the Breach
- If the breach poses a high risk to individuals, it must be reported to the Information Commissioner's

Office (ICO) within 72 hours.

- The Academy must notify affected individuals without undue delay if the breach is likely to result in serious harm.
- Investigation and Resolution
- Document how the breach occurred and identify corrective actions.
- Implement additional security measures to prevent future breaches.
- Review and Lessons Learned
- Conduct a post-incident review to identify weaknesses in data security.
- Update policies and train staff to mitigate risks.

8. The Subject Access Request Procedure

- See details on 'Manifestly unfounded and Excessive Requests' September 2019 at www.ico.org.uk

- Requests by individuals (or their representative) for copies of their own information must be in writing and supported by significant proof of identity. The following originals (not photocopies) are suggested:

- Passport
- Driving License; or
- Birth/Marriage Certificate

- The need to check and verify the identity of the requester can be particularly important where that person is a child or someone is purportedly making the request on behalf or in respect of a child.
- Enquirers should make a Subject Access Request using the exemplar format as a guide adding exactly what information is required (Appendix B).

- In the event of a Subject Access Request (SAR), the Principal as DC will prepare and direct all relevant information. This is also to ensure compliance within timescales (see 8.5).

- Information must not be deleted or disposed of, after the receipt of a request, unless requested by the subject. Subjects have the right to have incorrect or inaccurate information corrected. Deleting information constitutes a new offence without permission.

- Subject Access Requests will be supplied without undue delay or within one month. Where an investigation of a member of staff has commenced and that member of staff has requested Subject Access, the processing of the request should be undertaken as quickly as possible. In the event that a complaint is received regarding a Subject Access Request, the complaint will be addressed following the Academy's Complaints Procedure. Records of proceedings and decisions made will be kept in order to provide evidence for any external review of the complaint by the Information Commissioner's Office.

- Requests for personal information held by the Academy about an individual may result in the Trust seeking clarification from the requestor, for example to specify an area of information required, services or timescales. In cases where clarification is sought, the clock stops until the clarification is received and then restarts from where it left off.

9. Training

- All employees in organisations with over 250 staff, require training on the UKGDPR and personal information handling. Bay Learning Academy doesn't meet this staffing number but will provide training for those staff that handle personal information. Training is seen as one measure to help maintain compliance with the UKGDPR.

10. Security of Personal Data

- Unacceptable use includes:

- unauthorised access to personal information
- unauthorised disclosure of personal information
- unauthorised use of personal information, e.g. use of which the data subject has not been informed/consented to as in UKGDPR Law, section 2, page 48 and the Fair Processing Notice); and
- non-adherence to the Academy's policies and local authority's information-sharing protocols

- Employee, client or learner personal information must not be used for:

- any illegal purpose
- any purpose which is inappropriate in the workplace by virtue of the fact that it may cause embarrassment or distress to another person or may bring the Academy into disrepute; or
- any purpose which is not in accordance with the employee's role or job description

- (This is not an exhaustive list).

- Employees are required to notify the Principal (Data Controller), if they become aware or suspect that personal information is being misused or handled inappropriately.

11. Non-Compliance with Legislation & Policy

- The Principal is responsible for ensuring that employees' responses to requests for personal information remain appropriate and are in accordance with this policy and the UKGDPR.

- The Principal must ensure that instructions they give to employees, relating to requests for personal information and the processing of personal information, comply with UKGDPR and trust policy.

- Employees need to be aware that arrangements need to be in place that avoid parental and visitor contact with personal information to which they do not have a right.

- All employees must be aware of their own obligations with regard to the disclosure and the processing of information.

- Employees not complying with this policy or legislation will have matters reviewed and may be dealt with under the Academy's Disciplinary Procedure.

Contact details:

Information Commissioner's Office (ICO)

Tel: 0303 123 1113 (local rate) or via "Live Chat" on www.ico.org.uk (search *'Contact Us')*
Fax: 01625 524510

Website address: www.ico.org.uk

By post: Head Office, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

By email: If your enquiry is about a new or existing notification under the GDPR 2016, please email icocasework@ico.org.uk or use the message box that appears on the Contact Us page. You may find it helpful to read more about notification and the need to notify before sending your enquiry.

Appendix A Definitions

(a)	**Personal Information**
	Information relating to a living individual who can be identified from that information or from other information in possession of the organisation. This is information that affects a person's privacy whether in their personal or family life, business or professional capacity and includes the name, address and telephone number of an individual. It will also include information on a person's medical history, an individual's salary details and includes expression of opinion about the individual and of the intentions of the organisation in respect of that individual. Personal information also includes CCTV images and photographs which enable the identification of an individual
(b)	**Special Categories of Personal Information**
	Is defined in the Act as racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sex life, criminal convictions (see update November 2019 www.ico.org.uk)
(c)	**Data Subject**
	Any living individual who is the subject of personal information held by an organisation e.g. a learner, parent, member of school staff, council employee, agency worker, casual worker, customer, client, member of the public, partnership worker, councillor
(d)	**Processing**
	Any operation relating to information including: organising, retrieving, disclosing or otherwise making information available, deleting, obtaining, recording, altering, adding to, or merging
(e)	**Third Party**

	Any individual or organisation other than the information subject, the information controller or its employees or agents

APPENDIX B

Exemplar proforma for making a Subject Access Request

[Enter date]

Principal Leila Goring
Bay Learning Academy
leila@baylearning.academy

Dear Sir or Madam

Subject access request

[Include your full name and other relevant details to help identify you].

Please supply the personal data you hold about me, which I am entitled to receive under data protection law, held in:

[Give specific details of where to search for the personal data you want, for example:

- my personnel file;
- emails between 'person A' and 'person B' (enter dates from and to including years)
- the CCTV camera situated at ('enter location') on (enter date and times) and
- financial statements (enter details) held in account number (enter details)

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

[If relevant, state whether you would prefer to receive the data in a particular electronic format, or printed out].

It may be helpful for you to know that data protection law requires you to respond to a request for personal data within one calendar month.

If you do not normally deal with these requests, please pass this letter to your data protection officer or relevant staff member.

If you need advice on dealing with this request, the Information Commissioner's Office can assist you. Its website is ico.org.uk, or it can be contacted on 0303 123 1113.

Yours faithfully [Signature]