Broadway Academy Trust Policies

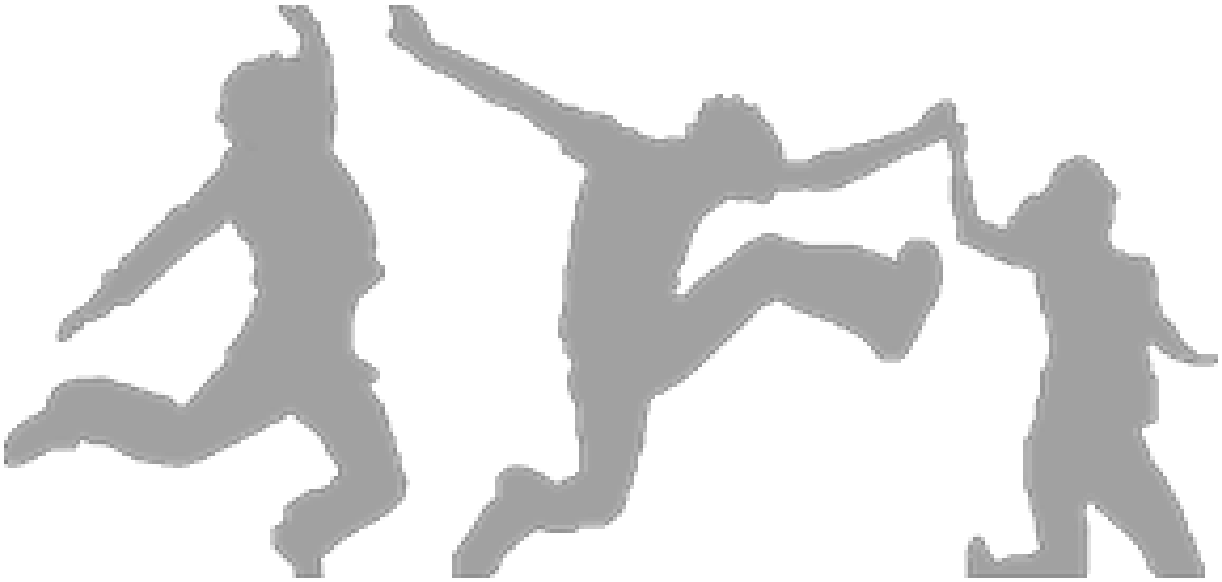
Our Children. Our Community. Believe it can be done!

Data Protection Policy

Approved by: Finance, Audit and Premises Committee

Date approved: June 2026

Next review date: June 2027



Contents

1. Introduction

1.1 This policy sets out how Broadway Academy Trust will ensure that all personal data is dealt with securely and in accordance with the Data Protection Act 2018, UK General Data Protection Regulation (GDPR). It will apply to all data held by the school regardless of the way it is used, recorded and stored and whether it is held by the school in paper files or electronic form.

1.2 The General Data Protection Regulation (GDPR) forms part of the Data Protection Act 2018. This regulation identifies certain principles that any organisation who stores or processes 'Personally Identifiable Information' must be able to demonstrate compliance with. The GDPR applies to all electronic and manual data files containing personally identifiable information (PII) or sensitive data.

1.3 Broadway Academy Trust collects and uses certain types of personal information about students, parents, staff, volunteers, governors, job applicants and other individuals who come into contact with the Academy in order to provide education, employment and other associated functions. The Academy is required by law to collect and use certain types of information to comply with statutory obligations related to education, safeguarding and employment.

1.4 This policy has been put into place to ensure all staff and governors who process PII in the Academy understand the scope of the regulation, how it affects them, and the working practices that must be employed on a day-to-day basis in order to safeguard the personal information of individuals held and used within the Academy.

1.5 Broadway Academy Trust will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties and that all personal information is held securely and is not accessible to unauthorised persons. All staff will be made aware of this policy and their duties under the GDPR.

2. Legislation and guidance

2.1 This policy meets the requirements of the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018).

2.2 It is based on guidance published by:

- The Information Commissioner's Office (ICO)
- Department for Education's (DfE): Data Protection in Schools (2024)
- DfE's: Keeping Children Safe In Education (2024)

2.3 In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Data Breach: *a breach of security leading to data being lost or stolen, destroyed or changed without consent or accessed by someone without permission. Data breaches can be deliberate or accidental*

Data Controller: *a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. The school is a data controller for the purposes of GDPR.*

Data Processor: *a natural or legal person, public authority, agency or any other body that processes personal data on behalf of the data controller. This applies to third party organisations who process data on behalf of the school.*

Data Protection Lead (DPL): a *nominated person with first point of contact responsibility for addressing data concerns and breaches and for liaising with the DPO*

Data Protection Officer (DPO)*: a person who is tasked with helping to protect personally identifiable information and helping an organisation to meet the GDPR compliance requirements. Ultimate accountability for compliance sits with the Governing Body and Headteacher and CEO.*

Data Subject: *an identified or identifiable living individual whose personal data is held or processed. In relation to school this includes, staff, parents, carers, students, volunteers, governors, visitors etc.*

ICO: *Information Commissioners Office (Supervising Authority in the UK)*

Personal Data – *examples of personal data include a name or title; contact details; information about behaviour and attendance; assessment and exam results; staff recruitment information and references.*

Personally Identifiable Information (PII) – *any information relating to an identified or identifiable, living individual.*

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. School specific data will also include information about safeguarding, pupil premium, special educational needs and disabilities, looked after children and children in need.*

Subject Access Request – *a right that a person has to obtain a copy of information held about them by the organisation*

4. Roles and responsibilities

4.1 This policy applies to all staff employed by the Academy, governors and external organisations or individuals working on its behalf. Staff who do not comply with this policy may face disciplinary action. Everyone in the Academy is responsible for protecting personal data.

4.2 Governing board - has overall responsibility for ensuring that the Academy complies with all relevant data protection obligations, monitors data protection performance, ensures security measures are appropriate to keep data protected and cyber security is considered within the continuity plan.

4.3 Headteacher and CEO - acts as the representative of the data controller on a day-to-day basis.

4.4 Senior leaders - are responsible for deciding how the Academy maintains security and how data is shared, setting policies for the use of data and technology, making sure contracts with third-party processors are relevant and supporting staff with annual staff training.

4.5 Data protection officer – The Academy has appointed a suitably qualified Data Protection Officer (DPO) who is provided to the school by SIPS Education, and is contactable via gdpr@sips.co.uk or 0121 296 3000

4.6 Designated Data Protection Leads (DPLs) within the Academy act as first points of contact. The Data Protection Leads are:
Stuart Carroll, Deputy Head Teacher (student data)
Sarah Bidwell, HR Director (staff data)
David Titchener, IT Director (IT systems and data)
Parmjit Hay, Clerk to the Governors (Governors' data)

4.7 All staff - Staff are responsible for:
- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the relevant DPL or 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 or near miss
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they are commissioning new systems or software with data collection implications, so that a data protection impact assessment can be carried out (see appendix B)
  - If they need help with any contracts or sharing personal data with third parties

5. Data Protection principles and how the Academy complies as a data controller

5.1 In accordance with the obligations placed upon the school as a Data Controller, personal data will be processed in accordance with the Principles of GDPR. The following section outlines how Broadway Academy processes personal data in line with the GDPR guiding principles.

	Data Protection Principles	**How the Academy Will Comply**
1.	Legality, Transparency and Fairness *The Academy will only process personal data, where it is able to demonstrate that it has a 'lawful basis' for the processing activity. Personal data will be processed fairly, and the Academy is open and honest about the uses of personal data.*	A data mapping document is a 'live' document that records all data processed by the Academy. A 'Lawful Basis' is recorded against each data set to evidence and record a legal reason for collecting, processing, sharing, storing, and destroying data. The data mapping document is held by the Strategic ICT Director. All staff will be required to assist periodic reviews of the data mapping document to ensure all data sets currently in use within the school have been considered, captured, and a lawful basis for processing has been identified on each occasion. A Privacy Notice details the Academy's use of personal data, including what PII is held by the Academy, how it will be stored, the organisations that data will be shared with, the lawful basis for processing and how long the data will be held prior to destruction.

		Our data mapping document informs the content of our privacy notices. It also contains information regarding how a data subject (e.g. student, parent, member of staff etc) can access their data, which is stored and processed by the Academy. In accordance with the principal of transparency, the Academy has developed and will maintain privacy notices for different categories of data subject. These outline the categories of data captured, the purpose of processing and if the information is shared with third party organisations. Privacy notices for students/ parents/carers, staff/volunteers, governors and visitors are available on the Academy website and paper copies can be made available from the administration office. A copy of the relevant privacy notice is also included in the Academy's admissions packs and staff induction packs. **A Data Subjects' Rights** Under the GDPR, data subjects have the following rights with regards to their personal information: 1. Right to be informed about the collection and the use of their personal data 2. Right of access personal data and supplementary information 3. Right to have inaccurate personal data rectified or completed if it is incomplete. 4. Right to erasure (to be forgotten) in certain circumstances. 5. Right to restrict processing in certain circumstances 6. Right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across difference services. 7. Right to object to processing in certain circumstances. 8. Rights in relation to automated decision making and profiling. 9. Right to withdraw consent at any time (where relevant) 10. Right to complain to the Information Commissioner Individuals can submit a request to exercise the above rights to the Data Protection Lead in school. This may be done verbally or in written form. If staff receive such a request, they will immediately forward it to the Data Protection Lead, who will liaise with the Data Protection Officer as necessary. See section 8 for details of how a data subject can exercise their right to access their personal data.
2.	Purpose Limitation *Personal data should be collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.*	The data mapping document identifies the purposes for which processing takes place, the description of the categories of individuals and personal data, the categories of recipients of the data (e.g. third-party organisations with whom the Academy shares the data). Retention schedules for the personal data are also noted. Appropriate technical and organisational measures must be in place to safeguard personal data and ensure PII is only used for the purpose for which it was collected.

3.	Data Minimisation *The personal data must be 'Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'*	Data collection forms and processes will be regularly reviewed to ensure information requested is appropriate and not excessive. Data required by teaching staff will be used only for the purpose it is required to ensure data used is minimal. If a member of staff wishes to introduce the use of new technology that captures personally identifiable information, they will first speak with the Data Protection Lead in school who will ensure appropriate measures, including completion of a data Protection Impact assessment prior to approval of a project and identify the appropriate lawful basis. The data mapping document will be updated accordingly. Wherever there is any uncertainty about the level of information being requested from Data Subjects, a referral should be made to the Data Protection Leads and Data Protection Officer for further guidance.
4.	Accuracy *All reasonable steps will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.*	Data will be proactively and regularly checked to ensure it is as accurate as possible through a variety of measures: • Update data collection forms annually to enable parents/carers to verify and amend data held on the Arbor system, including emergency contact details; correspondence address; medical details of students etc. • Use of apps such as ParentApp to allow parents real-time access to update data held on Arbor • Reminders in Academy newsletters • Data updates at parents' evenings and student progress meetings (e.g. check attainment data in systems) • Checking the accuracy of data during contact with parents (e.g. admin, SEND, attendance, reception, pastoral) • Annual personal details update forms for staff to amend data held in Arbor • Free school meals tracking system checks and updates
5.	Storage Limitation *Personal data shall be kept in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.*	Retention periods for various data held in the Academy are recorded within the data mapping document. The Academy uses the Information Record Management Society Toolkit to establish appropriate retention periods, and data is archived and destroyed as set out in these guidelines. Personal data that is no longer required either due to it being out of date, inaccurate or in line with the school retention policy, will be disposed of securely. Records of disposal are maintained for accountability, ~~ie~~i.e. certificate of destruction from shredding companies or record log completed by school. Archived paper documents are stored securely in a designated archive Secure Store (located next to the Exams Office) or the Secure Store at the back of the dining hall (financial information only) and clearly marked with their retention deadline. Destruction of documents at the end of their lifespan is carried out by Administration or Finance staff by shredding documents on site or by depositing confidential waste in the secure waste box

		for collection by a confidential waste disposal company. A third-party assurance certificate will be obtained to provide school with sufficient guarantees that the company complies with data protection law. Electronic files are deleted appropriately in line with retention periods. Data within emails (either as text or attached documents) are identified by content and filed into the relevant system, where it is then stored and destroyed in line with retention periods.
6.	Integrity and Confidential (Security) *Personal data will be processed in a manner, which ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage, using appropriate technical or organisational measures*	The Academy expects all staff to comply with the following technical and organisational measures to safeguard data: ***(a) Artificial intelligence (AI)*** • Artificial intelligence (AI) tools are now widespread and easy to access. Broadway Academy recognises the benefits of AI tools in a work setting however staff are informed of the challenges and risks AI systems may pose. • AI software within official or licensed software will be used appropriately and reasonably to accomplish tasks. • If staff are planning to use a new AI system, staff will first inform the DPL and IT support of this intention. If applicable, informed staff will recommend alternative solutions that may offer a safer and more secure use of data. If alternatives are not known, staff may be asked to complete a risk assessment or data protection impact assessment prior to use. • To ensure that personal and sensitive data remains secure and mitigate risks of a data breach, no one will be permitted to enter confidential or sensitive information into unauthorised generative AI tools or chatbots (Co-pilot, ChatGPT, Gemini etc). Such information includes but is not limited to personal data (also referred to in GDPR as Personally Identifiable Information); commercially sensitive or confidential data; and credentials (e.g., passwords). • If personal and/or sensitive data is entered into an unauthorised generative AI tool, Broadway Academy will treat this as a data breach and will follow the personal data breach procedure in section 13. ***(b) Cyber Security*** • For more information, please refer to the IT policy available on the school website/upon request. • Measures such as encryption and access control are in place to prevent unauthorised access to the Academy network. • Cyber security training and briefings are shared with staff to raise awareness and keep staff informed of the risks and procedures in place to protect data • The cloud provider shares responsibility for the protection of data and assurances have been received. ***(c) Clear desk and clear screen***

		• Staff will observe a 'clear desk' policy, ensuring that documents which may contain personal or sensitive data are never left on display. • Paper documents containing any personal data will be secured in lockable storage at the end of the day or when rooms are left unattended. Where there are concerns over the availability of secure (lockable) storage, or clarification needed about what types of information need to be secured, staff should speak with a DPL who will liaise with the DPO if needed. • Data will not be displayed on noticeboards. • PCs, laptops, school issued Ipads and mobile phones must always be locked when workstations are unattended. PCs can be locked by hitting the 'windows' and 'L' keys. • Positioning of computer screens should ensure only authorised personnel are able to view sensitive or confidential information. This is particularly important within areas accessed by members of the public e.g. reception, or in shared workspaces and classrooms. Privacy screens will be provided where positioning of screens alone will not address data security. ***(d) Passwords and protection of hardware*** • Passwords for accessing systems must be complex enough to make it extremely difficult for third parties to break them. Passwords must be at least 8 characters long, with a mixture of 3 complex characters (upper-case, lower-case letters, numbers and symbols). • Passwords should be changed regularly (and compulsorily on a 90-day rotation) • Passwords will not be shared with any other member of staff / shared amongst other users or written down. • Academy mobile devices (phones, tablets and laptops) will be protected to the same high standard. Staff must: o activate the built-in security PIN and set this to the most secure level (if the device allows, this should be a secure password as above or fingerprint recognition rather than a 4-digit pin) o ensure they have a copy of phone and SIM IMEI numbers stored securely to allow deactivation in the event of loss. • Staff are personally responsible for any information accessed or disclosed on Academy devices, so it is imperative that passwords are kept safe and secure and not shared with anyone else. ***(e) Accessing and sharing information*** • Staff are requested not to access private email accounts in school on any Academy equipment. Academy emails and cloud data (on Virticad) can be accessed securely on personal devices, at home or onsite providing no data is download. • Staff should only use personal devices on site having completed and signed the Bring Your Own Device (BYOD) form. The exception to this will be where specific permission has been given in emergency situations. • When calling students during such an emergency, staff must take care to protect their and their colleague's privacy. Calls

		from teachers' mobiles may be necessary but staff should always block their number when communicating with parents or students. If asked, the standard school number should always be provided. • *It is important that employees understand the difference between **accessing** data (looking at or reviewing) via a mobile or off-site device and **downloading/saving** data (this will save a copy of the information onto the mobile device you are using). Data should **not** be downloaded or saved to a mobile or offsite device unless you can justify this action with a clear business case for doing so. Once the data is no longer required on the device it must be deleted immediately.* • All emails on and off site with attachments will be encrypted by default. Shared files via email are only available to Broadway Staff, unless special permission is agreed (*). • All USB sticks plugged into Broadway Academy systems and equipment will be encrypted by default unless special arrangements are made. (* Exception from encryption is only available to staff members with unique requirements, such as the exam officer. Any request for non-encrypted data will be handled by the Strategic ICT Director.) • Staff should be aware that work email accounts and files may be accessed by the academy if required to support management of the school e.g. in the case of staff absence or handover. ***(f) Sharing of Personally Identifiable Information*** There will be occasions when it is necessary to share information with others, in which cases the following must be observed: INSIDE THE ACADEMY: • If information is of a confidential, sensitive or personal nature, it must be handled correctly i.e. it is only sent, shared, viewed or edited by authorised Academy personnel. • Do not copy people into emails if they do not require access to the information contained within. • Delete sensitive, confidential or personal information once it has been used for the purpose it has been collected and is no longer required. • Minimise the use of sending attachments to other staff on site and instead share documents via One-drive and SharePoint. Office documents can be shared directly with the correct staff member from within the application. • Avoid printing out documents which can be accessed in shared drives; if documents are printed, they must be disposed of correctly in confidential waste bins located in the administration office. OUTSIDE THE ACADEMY: • Where more than one piece of personal, sensitive or confidential data is to be sent, one of several methods can be used. If in doubt, check with a DPL or seek advice from the DPO. • Use secure transmission: where possible, use recognised methods such as WebEx.

		• Never send personal data within a normal email. If email is the only method of transmission available, ensure the information is included in a password protected document. The password must be agreed with the email recipient in advance, and via telephone, not in another email. Never include the password in the email to which the password protected document is attached, nor send the password via another email (if the first email is intercepted, then the second could also be). • Ensure that a request for data is a valid one and that only the required data is provided. Always check why people require the data they ask for – if in doubt check with the DPL before sending. • Make sure that the data is up to date. Check the validity and accuracy of the data before sending • Academy emails should never be sent to public email addresses (e.g. Hotmail, Gmail etc.) regardless of what they contain, unless this has been clearly identified by the recipient as their business email address. • When sending information (including letters) via post, the following must be adhered to: o Ask a second person to check the address is correct before sending. Pay particular attention to numbers as these can be transposed, but be aware the responsibility for accuracy is still with the sender not the checker o Consider using window envelopes if the address is on the letter to avoid transcription errors or use typed labels to avoid errors arising from handwriting legibility. o DO NOT USE window envelopes if the heading of the letter (which may be revealed in the window) contains sensitive information (e.g. disciplinary investigation, exclusion hearing) o Ensure that envelopes are securely sealed. Use additional methods such as sticky tape, glue or staples if necessary o Double check that no additional information has been included that is not relevant e.g. something mistakenly attached. Check that any data is valid and accurate. o If a request is received from an outside agency, such as the Police, this should be referred in the first instance to the DPL. ***(g) Storing Data on Portable External Devices*** • It is not recommended that staff or students store data on any such device. • The loss of any device that can send, store or retrieve data must be reported to the IT Manager and the DPO immediately • Devices that can transmit and receiving data information, such as smartphones, should only be used for the purposes for which they were supplied and must be protected by a strong secure password. • Anyone who uses portable devices to access or store data is responsible for the information which is transported within. This includes USB flash memory devices (“memory sticks”), laptops, external hard disk drives, mobile phones, tablets. Be aware of

		devices that can access information, such as emails, which could contain sensitive data • Any memory stick/portable device that you use for the transport or storage of personal or sensitive nature must be encrypted to an appropriate standard and approved for use by the IT Manager/ DPL. • All portable devices must be encrypted, and care must be taken to safeguard the equipment against loss or damage. The password used to encrypt information must not be written down and must never be stored or transported with the device. Please be aware an encrypted memory stick/portable device will ALWAYS ask you for a password before use. • Any school laptop with could be used off site will be encrypted and will therefore require additional passwords to gain access. It is essential that this or any other password is not stored, with, on or around the actual device. • Any storage devices no longer required which may contain information that is surplus to requirements or any device that is in need of secure disposal should be returned to the IT staff or the IT DPL, in person. • Media such as CDs or DVDs which contain data and are no longer required must be physically destroyed. If you do not have the means to do this, pass them to the IT Department/IT DPL stating clearly that they contain sensitive information ***(h) Storing data in Paper and Manual filing systems*** • Paper based (or any non-electronic) information must be assigned an owner who takes responsibility for its storage and protection. • A risk assessment should identify the appropriate level of protection for the information being stored. Paper and files in the Academy must be protected by one of the following measures: • Filing cabinets that are locked with the keys stored away from the cabinet • Locked safes • Stored in a secure area protected by access controls Depending on the content of the sensitive data contained within papers and files, the appropriate member of staff will be responsible for the storing and protecting of the data in line with the secure filing system process. ***(i) Security of Equipment and Documents Off-Premises*** • Information storage equipment, data, software or any documents containing personal, sensitive or confidential data should not be downloaded off-site without authorisation from the Head Teacher/CEO. • The following security guidelines must be adhered to for all equipment and documents taken offsite. They must: o not be left unattended in public places o not be left unattended in a vehicle unless the property is concealed from view and all doors are locked, windows and the roof closed and fastened, all security devices on the vehicle are in full and effective operation and all keys/removable ignition devices removed from the vehicle

- not be left open to theft or damage whether in the office, during transit or at home
- where possible, be disguised (e.g. laptops should be carried in less formal bags)
- be returned to the Academy as soon as is possible

(j) Physical Security

This section is related to building security and the level of care that will be taken when transporting computers or paper files outside of the building.

Data held by the school will be protected against the possibility that it could be stolen, lost or otherwise divulged by physical (or non-electronic) means. The following organisational security measures are in place to protect all sensitive, personally identifiable and confidential information:

- The Academy premises are protected by site security, door locks, RFID card locks and, in some secure locations, access codes. Codes must remain secure as these form part of the physical security procedures and help to keep personal, sensitive and confidential data safe
- Doors and windows must be locked when unattended and external doors (including loading/fire doors) must be locked when not in use
- All visitors must sign in at the main site reception using the photo ID system and receive a Visitor's Authentication Badge on the appropriate coloured lanyard.
- Visitors must record their date/time of entry/departure and person(s) being visited
- All Visitors should be supervised at all times and are required to wear the visible authorised ID on the appropriate coloured lanyard.
- If a visitor requests access to confidential data or computer systems, it is the employee's responsibility to ensure it is a legitimate request and data protection principles are not breached. If in doubt, please check with your DPL or the DPO.

(k) CCTV

- The Academy operates a CCTV system to monitor activities within and around school, to identify instances of criminal activity and to ensure the safety and wellbeing of the school community. The school do not need to ask the permission of individuals on the school site to record images on CCTV.
- The Academy will only operate overt surveillance and will display signs in the areas of the school where this is in operation. Covert surveillance (i.e. which is intentionally not shared with the individuals being recorded) is not condoned by the Academy.
- Any enquiries or complaints about the Academy's CCTV system should be directed towards the data protection lead in school in the first instance, who will investigate as required, and respond in accordance with the Academy's CCTV policy.
- For more details, please refer to the Academy's CCTV policy

		(l) Remote working In the event of Academy closure or any occasion that requires staff or students to work from home, the same data security principles should always be applied. Student details should be accessed remotely and never stored locally on any computer. Students should be aware that staff will contact them directly via the Academy cloud system (Arbor / Microsoft 365 and TEAMS) and should be encouraged to communicate back to staff in the same way.
7.	Accountability *Broadway Academy as data controller will be able to demonstrate compliance with the previous principles.*	• A Data Protection Officer is appointed with suitable knowledge and experience to fulfil the role and a direct line of report through to the Head Teacher and Governing Body for data protection related matters. The Academy's Data Protection Officer is provided by SIPS Education and is contactable via gdpr@sips.co.uk or 0121 296 3000. • On a day-to-day basis Data Protection Leads are the first point of contact (see section 4.6 for list); the relevant DPL will liaise with the Data Protection Officer for advice and guidance as required. • The Academy has clear procedures in place for handling a data breach and a Subject Access Request. • The DPO will undertake periodic monitoring to ensure compliance with the regulations. They will be informed of any suspected data breach and will help to investigate circumstances surrounding breaches and ascertain whether they are reportable to the ICO. • The DPO will be informed by DPLs of any Subject Access Requests made to the Academy and will assist in making the response to the Data Subject. • The Governing Body will be kept informed of ongoing compliance via reports to the Finance, Audit and Premises Committee which will include an overview of any data breaches that have occurred along with actions taken, and any Subject Access Requests received and responded to. • Academy staff are GDPR trained on an annual basis via an eLearning training platform. In addition to this, regular reminders to staff on the content and expectations of this policy and the procedures to follow to safeguard personal data is carried out.. • Regular Data Audits and reviews are undertaken to check the robustness of processes and systems for continued GDPR compliance.

6. Use of Personal Data

6.1 Broadway Academy Trust processes personal data on students, staff and visitors. Personal data for each individual will be processed in accordance with the principles in section 5.

6.2 In accordance with the principle of transparency, the Academy has developed and will maintain privacy notices for different categories of data subject. These outline the categories of data captured, the purpose of processing and if the information is shared with third parties. Privacy notices can be found on the Academy website at GDPR Privacy

Notice | Broadway Academy (broadway-academy.co.uk) for the following categories of data subjects:

- Students and parents/carers
- Staff and Volunteers
- Visitors and contractors
- Governors

6.3 Where the Academy is introducing new technologies or it is considered that the processing of personal data presents a high risk to the rights and freedoms of individuals, Data Protection Impact Assessments will be completed to ensure appropriate measures are put in place to safeguard data, prevent breaches and ensure compliance. A copy of the Data Protection Impact Assessment template is included at Appendix 1.

6.4 The Academy 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 necessary consent before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. (See section 7 for third party data processors)

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

6.6 Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

7. Third Party Data Processors

7.1 Where the Academy works with or uses third-party data processors, we will ensure we only appoint or work with suppliers or contractors who can provide sufficient guarantees that they comply with UK data protection law. This means that we:

- Use standard contract terms in our procurement arrangements to ensure data processors comply with UK data protection legislation
- Carry out due diligence checks on the data protection policies and arrangements of third-party data processors as part of the procurement arrangements, including receiving copies of their data protection policies
- Only share data that the supplier or contractor needs to carry out their service
- Carry out a data protection impact assessment as part of the process of introducing new or amending existing data sharing arrangements
- Review and record third party providers on the Academy's data mapping document, including identifying the data sets that are shared with them and recording assurances received of how the providers process and protect data shared by the academy. These are stored centrally and recorded on the data mapping document. The data mapping document should be reviewed annually.

8. Biometric Recognition System

8.1 In some instances, the Academy may wish to capture and use individuals' biometric data to operate automated systems. Biometric data is personal information about an individuals' physical or behavioural characteristics that can be used to identify that

person. This can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

8.2 At Broadway Academy, we currently operate biometric systems in the following ways, and for the following purposes:

- Using student fingerprints or facial recognition to access school meals as an alternative to paying with cash
- Using student fingerprints to access library service
- Using staff members' fingerprints or recognition to access school meals as an alternative to paying with cash

8.3 The ICO consider all biometric data to be classed as personal data, and as such will be processed in accordance with the principles of the General Data Protection Regulation 2018, and Data Protection Act (2018). The use of student biometric data in automated biometric recognition systems, will also be undertaken in accordance with the relevant sections of the Protection of Freedoms Act 2012.

Use of Student Biometric Data

8.4 In any situation where the Academy wishes to use students' biometric data, we will ensure that Parents / Carers are notified of our intention to use such data as part of an automated biometric recognition system. We will do this either before any new system is put in place, or before students first use an existing system.
Consent will be obtained from at least one parent / carer before the Academy takes any biometric data from their child and process it. We will not process students' biometric data in the following circumstances:

- If the student (verbally or in written format) objects to the use of their biometric data, or refuses to take part in the processing (irrespective of any consent given by the parent / carer)
- Where we have not received written consent from at least one parent to the processing
- Where a parent has objected in writing to the use of biometric data, even if other parent has given written consent.

8.5 We will provide alternative ways to access relevant services, where parents / carers or students have chosen not to use biometric recognition systems.
Consent can be withdrawn by parents/carers and students at any time, and in such circumstances, we will ensure that any relevant data already captured is deleted.

Use of Staff Biometric Data

8.6 Similarly, where the Academy wishes to use staff members' (or other adults') biometric data as part of a recognition system, we will first obtain your consent to do so and before you take part in the system.
If you do not wish to have your biometric data captured, we will provide an alternative means for you to access the relevant service. You may also withdraw consent at any time, and in those instances, we will delete any relevant data already captured.

9. Photographs and Videos

9.1 The Academy may take photographs and record images of individuals as part of activities. Such images may be used for:

- Within the Academy on notice boards and in newsletters, brochures etc.
- Online on the Academy website or social media
- Outside of the Academy by external agencies such as the school photographer, newspapers or for media campaigns

9.2 In order to do this, we will obtain written consent from parents / carers before we take photographs or videos of their child. We will do this when the student starts at Broadway Academy and update annually. When we seek consent, we will clearly explain how the photographs and/or videos are to be used.

9.3 Parents/carers and students have the right to withdraw consent at any time, upon which we will delete any images already taken and we will not distribute those images further.

9.4 As part of our 'public task,' we may take a photograph of a student without requesting consent from the parent/carer. This would be in circumstances where identification of a child with an existing medical condition/allergy is required to meet the needs of the student and to keep them safe.

9.5 Where photographs and/or videos are taken by parents / carers at Academy events for their own personal use, the requirements of data protection legislation do not apply. However, we do ask that, should such photos / videos capture images of other students in addition to their own child, they are not shared in any public way (including on social media sites) for safeguarding reasons unless all relevant parents / carers have agreed to this.

10. Virtual Teaching and Learning

10.1 Staff in emergency situations could be asked to teach remotely. Hardware such as laptops and cloud systems such as the Arbor pupil portal will be provided by the Academy to handle all assignment of lessons and communication to students. Actual live lessons could be delivered via webcam software but when doing so teachers should ensure:

- Their web cam only displays the teacher with as blank as possible background – virtual backgrounds should be encouraged.
- Whilst using webcam software the only visible screen should be that of the teacher. No broadcast of student web cams should be permitted.
- All live web cam lessons with students should be recorded and automatically secured in a private storage.

11. The rights of the Data Subject

11.1 Under data protection law, data subjects have the following rights with regards to their personal information:

i. to be informed about the collection and the use of their personal data
ii. access to personal data and supplementary information
iii. to have inaccurate personal data rectified, or completed if it is incomplete
iv. to erasure (to be forgotten) in certain circumstances
v. to restrict processing in certain circumstances
vi. to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across difference services.
vii. to object to processing in certain circumstances
viii. rights in relation to automated decision making and profiling.
ix. to withdraw consent at any time (where relevant)
x. to complain to the Information Commissioner

11.2 Individuals can submit a request to exercise the above rights to the Data Protection Lead in school. This may be done verbally or in writing. If staff receive such a request, they will immediately forward it to the Data Protection Lead, who will liaise with the Data Protection Officer as necessary. See section 13 for further information how a data subject can exercise their right to access their personal data.

12. Subject Access Requests

12.1 Individuals have a right to make a 'subject access request' to gain access to personal information that the Academy holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purpose of the data processing
- The categories of personal data concerned
- With whom the data has been, or will be, shared
- For how long the data will be stored, or if this is not possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restrictions, 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
- The safeguards provided if the data is being transferred internationally

12.2 It is important to note that a child's personal data is just that – their data – and does not belong to their parent / carer. As such, if a parent or carer wishes to make a subject access request for data relating to their child, the student needs to have given their consent dependent on their age and level of understanding.

12.3 The age of 13 is used as a guide to determine when a child is generally likely to be mature enough to understand their rights, and accordingly any requests for their personal data from this age onwards would generally be expected to come from the student themselves. For students below this age, it is less likely that they will fully understand the implications of SARs, and so it would normally be acceptable for the request to come from the parent / carer.
However, both of the above situations above are used as a guide only, and each request (and requestor) will be judged on an individual case by case basis.

12.4 Subject access requests can be submitted in any form to any member of staff within the Academy. However, the Academy may contact the requester for more details in order to respond to requests appropriately. When staff receive a subject access request, they will forward to the relevant data protection lead within the Academy immediately. The data protection officer will also be advised to ensure appropriate support is provided to the Academy to fulfil the request.

12.5 Parents can also contact the data protection leads within the Academy to make a subject access request. Alternatively, see Appendix B for a form to complete in order to submit a Subject Access Request.

12.6 When responding to requests, the Academy may:

- contact the individual via telephone to confirm the request has been made by them
- ask the individual to provide further details so that the Academy can verify and confirm the data required.
- request two forms of identification of the individual. Proof of address will also be verified.
- if a third party is requesting data, written authority or a power of attorney will be verified.

12.7 Requests will be responded to within 1 calendar month from receipt of the request. If the 30th day falls on a weekend or bank holiday, the pack will be made available on the next working day. However, if additional information is required in order for the Academy to fulfil

the request, the response period will be from receipt of all information obtained. This includes receipt of proof of identity and proof of address where relevant.

12.8 The response to the Subject Access Request will be made in the same format as the request was received unless the preferred format has been included in the request. For example, if the request is made by email, the data will be received electronically.

12.9 Based on the complexity of the request and in line with Article 12 (3) GDPR, the period in which to respond to a Subject Access Request may be extended up to 3 calendar months if required. In such instances the Academy will liaise with the Data Protection Officer and liaise with the requester to advise of the response time or any delays at the earliest opportunity.

12.10 Data provided to the requester may contain details of other individuals and therefore such data will be redacted (blanked out) to protect those individuals' identities and personal data. Details contained within the documents will pertain to the appropriate individual only.

12.11 When responding to the request, the Academy may decide not to disclose information for a variety of reasons, including if it:

- would have an adverse effect on the rights and freedom of others
- is information that might cause serious harm to the physical or mental health of the student or another individual
- is information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- is information contained in adoption and parental order records
- is information which may be used in legal proceedings
- would include personal data relating to another individual, where the Academy cannot sufficiently anonymise the data to protect that individual's rights, the Academy does not have their consent to release that individuals' data, and it would be unreasonable to proceed without such consent.

12.12 If a request is determined to be 'unfounded or excessive, the Academy has the right to refuse the request, or in some cases, charge a reasonable fee to cover the administrative costs of responding to the request.
If the Academy refuses a request, we will inform the individual of the reasons why and advise them of their right to complain to the ICO, if they wish to do so.

13. Data Breaches

13.1 The Academy will make all reasonable endeavours to ensure that there are no personal data breaches. The Academy has robust procedures in place to deal with any personal data breach and will notify the ICO where we are legally required to do so. Data subjects will be notified in instances where the rights and freedoms of such individuals has been compromised. The Academy will work with the Data Protection Officer to address a breach and Academy processes will be reviewed to mitigate risks if it is appropriate to do so.

13.2 If any member of staff becomes aware of a data breach, they must report it to the relevant Data Protection Lead as soon as possible, who will take advice from the DPO. Staff should also report any near misses so that we can learn from these and use them to inform future revisions to data protection policies and procedures.

13.3 The Academy will keep a record of all breaches and investigate them to an appropriate level, in order to ascertain what can be learnt from the circumstances surrounding each breach, and to use this to review procedures with the aim of preventing a similar breach occurring again.

13.4 Where breaches are reportable, the report must be submitted to the ICO within 72 hours of the Academy becoming aware of the breach; therefore it is crucial the Data Protection Lead is notified of any potential breaches immediately.
A near miss will also be reported to the DPL so that the school can learn from these and use them as a way of informing future revisions to our policies and/or procedures for data protection.
The Data Protection Leads will meet regularly to keep all data protection issues under review and to ensure policy and practice is up to date.

14. Contact Details

14.1 Subject Access Requests, concerns about a data breach or general queries in relation to data protection within the Academy should be directed to the relevant Data Protection Lead within the Academy:

- Stuart Carroll, Deputy Head Teacher (student data) - s.carroll@broadway-academy.co.uk
- Sarah Bidwell, HR Director (staff data) – stzsb@broadway-academy.co.uk
- David Titchener, IT Director (IT systems and data) – david.titchener@broadway-academy.co.uk
- Parmjit Hey, Clerk to the Governors (Governors' data) – parmjit.hey@broadway-academy.co.uk

14.2 Further concerns, questions or complaints can be discussed with the Data Protection Officer at gdpr@sips.co.uk or telephone number 0121 296 3000.

14.3 After contacting the Data Protection Lead and Data Protection Officer, if a data subject remains dissatisfied with the assistance that they have received, they can make a formal complaint to the Information Commissioners Office.
The Information Commissioner can be contacted at:
Information Commissioners Office, Wycliffe House Water Lane Wilmslow Cheshire, SK9 5AF
Tel: 0303 123 1113
Website: https://ico.org.uk

15. Links to other policies

15.1 This data protection policy is linked to the following Academy policies

- Acceptable use of the Internet and Social Media policy
- CCTV policy
- Freedom of information policy and publication scheme
- Protection of Biometric Information policy

Appendix A - Data Protection Impact Assessment Template

Data Protection Impact Assessment (DPIA)

School	
Completed by:	
Date	
Name of Project	
Nature of the project *(delete as appropriate)*	New Project Significant Changes to an existing process or project

Why is a DPIA Required? Why have you identified the need for a DPIA? Explain what the project aims to achieve and what type of processing of data it involves (you could attach the project proposal).

The final outcomes of this assessment should be integrated into the project plan.

Describe the processing of the data • How will you collect, use, store and delete data? • What is the source of the data? • Will you be sharing data with anyone? • You might find it useful to refer to a flow diagram or other ways of describing data flows • What types of processing identified as likely high risk are involved?
Describe the scope of the processing: • What is the nature of the data, and does it include special category or criminal offence data? • How much data will you be collecting and using? • How often? • How long will you keep it? • How many individuals are affected? • What geographical area does it cover?
Describe the context of the processing: • What is the nature of your relationship with the individuals? • How much control will they have? • Would they expect you to use their data in this way?

• Do they include children or other vulnerable groups? • Are there prior concerns over this type of processing or security flaws? • Is it novel in any way? • What is the current state of technology in this area? • Are there any current issues of public concern that you should factor in? • Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
Describe the purposes of the processing: • What do you want to achieve? • What is the intended effect on individuals? • What are the benefits of the processing – for the school, and more broadly?
Consider how to consult with relevant stakeholders: Describe when and how you will seek individuals' views – or justify why it is not appropriate to do so. Who else do you need to involve within your school? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
List the source of risks and potential impact on individuals here. For the likelihood and severity of harm and the overall risk, use one of the following terms listed in the relevant column.	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in table above				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Item	Name/position/date	Notes
Measures approved by:		Integrate actions into the project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, (Measures table) before processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

APPENDIX B Subject Access Request Form

BROADWAY ACADEMY

SUBJECT ACCESS REQUEST FORM FOR PARENTS/STUDENTS

Name	
Contact Address	
Contact Telephone Number	
Name of student data is required for	
Student's Date of Birth	
To ensure a timely response, please provide as much detail as possible about the data you require.	

Identification requirements - In order for data to be provided and to satisfy all parties that data is being shared with appropriate persons, Broadway Academy Trust will require identification of the requester, including proof of address.

If you are a third-party requesting data relating to an individual, written authority from the parent/student will be required. Where a power of attorney is in place, evidence of this will be requested prior to the release of data.

Response times - Upon receipt of the completed Subject Access Request and all information required to fulfil the request, Broadway Academy Trust will provide a response to you within a calendar month in line with GDPR. Should a request be deemed complex, the Academy will advise you of this and provide a response period, which can be up to 3 calendar months.

Please return the request to Stuart Carroll, Deputy Headteacher s.carroll@broadway-academy.co.uk or gdpr@broadway-academy.co.uk or to: Broadway Academy, The Broadway, Perry Barr, BIRMINGHAM B20 3DP

Signed:_____ Date:_____