Data Protection Policy (GDPR)

Published Date: April 2018

Policy Version Number:	002			
This policy applies to:	Staff, Students, Parents, Suppliers, Stakeholders			
Related Documents/ Policies:	Academy Privacy Statements Record Retention Policy Freedom of Information Policy IT Security Policy			
Author:	Pamela McIlroy			
Area:	SLT			
Changes made/Reason for Review:	Update for GDPR			
Approval required by (please tick):	A&R ✓	F&R	Trust	Rem
Approved by/Date:	SLT (All Academies)		w/c	
	LJC (if applicable)			
	Committee (A&R)		3/7/19	
	Trust Board		22/10/19 (ratified only)	
Date of Next Review:	July 2021			
Equality Impact Assessment	This Policy has been reviewed against equal opportunities legislation with regard to age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage and civil partnership and pregnancy and maternity and has no identified adverse impact (direct or indirect) on minority groups			

CONTENTS

1 INTRODUCTION

The General Data Protection Regulation (GDPR) is EU-wide legislation which enhances the existing Data Protection Act (1998) in determining how personal data is processed and kept safe and the legal rights individuals have in relation to their own data.

Organisations processing data must comply with the following GDPR principles. Personal Data should be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified explicit and legitimate purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection.

Data Controllers are required to show how they comply with the Act by having technical and organisational measures in place, including policies, staff training, documentation and audits. Data Controllers and Processors can receive significant fines for non-compliance.

GDPR also provides the following rights for individuals:

- The right to be informed
- The right of access
- The right of rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The Pinnacle Learning Trust (the Trust) and the Academies and Colleges within it (referred to in this document as the Academies) are Data Controllers. The Trust shall take all reasonable steps to implement appropriate technical and organisational measures to demonstrate that it is compliant with the Act and ensure that data is processed in accordance with the legal requirements. Processing is defined as "any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

Academies may have contracts with other organisations to process data. These suppliers are Data Processors and they have a legal duty to process data in line with the Act and maintain records of personal data and processing activities. They are responsible for any breach in the data processing. However, the Academy is responsible for ensuring that contracts with Data Processors are compliant with the law and the Trust's Data Protection Policy.

The policy does not form part of any employee's contract of employment and may be amended at any time.

Further information about the GDPR is available from the Information Commissioner's Website www.ico.org.uk.

2 POLICY STATEMENT

This Policy sets out the basis on which the Trust and its Academies will process any personal data they collect from data subjects, or that is provided to them by data subjects or other sources. It includes the responsibilities of staff within the Trust in complying with GDPR, as well as the rights of individuals whose data is being processed.

The Data Protection Officer (DPO) for the Trust is Corinne Walker. Their responsibilities in this role are detailed in section 3 below. Each Academy will have a nominated person responsible for the compliance of this policy within their Academy. Any questions about the operation of this Policy should be referred to the Data Protection Officer.

2.1 Personal Data

Personal data means "any information relating to an identified or identifiable natural person ('data subject')". An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier

or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

GDPR applies to both electronic data and manual filing systems. Personal data that has been pseudonymised may still be subject to this Act depending on how difficult it is to attribute the pseudonym to the individual. Personal data covers both facts and opinions about an individual.

2.1.1 Special Categories of Personal Data/Sensitive Data

Special categories data is entitled to special protection under the Act, and will only be processed by the Academy with the explicit consent of the appropriate individual, or as otherwise permitted by the Act. The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Special categories include:

- racial or ethnic origin
- political opinion
- religious or philosophical beliefs
- trade union membership
- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation.

2.2 Data Processed by the Trust and its Academies

During the course of the Trust/Academy's operation it collects, stores and processes personal data about employees, students, parents, suppliers and other third parties. The Trust/ Academy will process data which is necessary for compliance with its legal obligation set out by the Department for Education. Other data may be processed in order for the Academy to undertake its day to day functions in terms of employment, education and management. Privacy Statements will inform individuals of how their data is being processed and the legal basis for processing (see section 2.3).

The Academy will consider the following when making decisions to process data or when introducing a new initiative or software:

- What information?
- Why it is needed?
- Who will have access to the information?
- Where will it be held?
- How long will it be kept?
- What if consent is not given?
- Who will data be shared with?

Each Academy will keep an up to date Data Asset Map which will contain the information listed above.

In certain circumstances individuals have the right to restrict processing or to object to processing. In most cases this will not apply to the data processed by the Academy, however if the Academy receives a request from an individual they should consult with the DPO.

2.2.1 Students

Students referred to in this document can be prospective, current or former students.

The Academy will process a wide range of personal data about students as part of its operation. The Academy receives personal data from the individual directly (or, in the case of students under 16, from parents). However in some cases personal data may be supplied by third parties (for example another Academy, or other professionals or authorities working with that individual), or collected from publicly available resources. Additional information will be generated and stored about students during their time at the Academy, such as attendance data, progress, course/timetable information, examination/test results and disciplinary records. Information about what data the Academy processes will be provided in the Privacy Statement. Students and/or their parents are required to sign a declaration to confirm they have read and understood the Privacy Statement on application or enrolment to the Academy.

2.2.2 Parents and Emergency Contacts

Parents are the parents, guardians or carers of prospective, current or former students.

The Academy will record the details of who has parental responsibility for students, plus information regarding parents' names, addresses and contact information in order to meet the requirement to keep parents of students up to the age of 18 informed of their child's progress, attendance, behaviour, etc. The Academy may also contact parents to keep them informed of what is happening at the Academy.

The Academy may also process contact details for Emergency Contacts who do not have parental responsibility.

2.2.3 Employees

Employees refers to applicants, current and former employees, including casual and agency staff, volunteers, Trainee Teachers and subcontracted employees, however the amount and level of data varies depending on the contract with the Trust.

The Trust will collect and process data about employees working for the Trust and its Academies. In most cases this will be provided by the individual, however in some cases personal data may be supplied by third parties (for example a previous employer or other organisation or agency), or collected from publicly available sources. Additional information will be generated and stored about employees during their time at the Academy, such as attendance and performance data. Information about what personal data the Trust processes will be provided in the Privacy Statement which staff are required to sign on application/induction to the Trust.

2.2.4 Other Stakeholders

The Academy will hold data relating to suppliers, subcontractors, and other stakeholders. The Academy will process any such data in accordance with its responsibilities under the Act.

Governors will be informed of how the Academy processes information about them in a Privacy Statement.

2.3 Privacy Statements and Consent

The Academy will publish a Privacy Statement for students and employees detailing how it obtains, stores, processes, shares and disposes of personal and sensitive data, and the reason for processing such data. The Privacy Statement will satisfy the individuals' right to be informed. Individuals will be required to agree to the data being used for the purposes identified on the Privacy Statement at the point of application/enrolment to the Academy or Trust. Privacy Statements are available on the Academy and Trust websites.

The processing of any data not contained in the privacy statement will require further information to be provided to individuals and consent, if necessary.

Consent is not required for every piece of data processed as long as the Academy fulfils the legal basis for processing such data. However where consent is required it must be freely given, specific, informed and an unambiguous indication of the individual's wishes. Therefore, the Academy will not assume consent, use opt out clauses or pre-ticked boxes. The Academy will retain copies of consent during the period of processing.

2.3.1 Parental Consent

The Children's Act states that parents have responsibility for decisions about their child's schooling until the age of 18. However, the rights under GDPR are those of the individual to whom the data relate. In most cases where students are under the age of 16, the Academy will rely on parental consent to process data relating to students (if consent is required under the Act) unless, given the nature of the processing in question, and the student's age and understanding, it is more appropriate to rely on the student's consent/agreement.

Students aged 16 and over will be required to give their own consent and will have rights under the Act relating to their own data. However, parents will be required to give consent to the processing of images of their child in relation to their course.

2.4 Accuracy of Data

The Academy will endeavour to ensure that all personal data held in relation to an individual is as up-to-date and accurate as possible. Individuals also have a responsibility to notify the Academy of any changes to information held about them. The Academy will regularly make personal data that has been provided by the individual available to those individuals (employees, students or their parents) for checking at least once a year.

An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the Act). In most cases an employee, a student or their parent who identifies incorrect information about them on the Academy record will simply notify the appropriate department to request that it is amended. The department must keep a record of who made the request, when it was received, when it was amended and by whom (ie an audit trail of changes to personal data). However in some circumstances the individual may feel that the matter needs to be brought to the attention of the DPO, in which case they should put this in writing to the DPO. Under GDPR, the Academy has to correct data within one month of notification, however it is in the Academies' interest to amend the data as soon as is reasonably practical. The DPO will formally respond to any request made to them in writing.

2.5 Access to Personal Data (Subject Access Request)

Individuals have the right under the Act to access personal data about them held by the Academy, subject to certain exemptions and limitations set out in the Act. Any individual wishing to access their personal data should put their request in writing to the DPO. Parents can make a Subject Access Request for students aged under 16 and for students 12 and under the request must be made by their parent. The DPO is required to verify the identity of the person making the request.

The Academy will endeavour to respond to any such written requests as soon as is reasonably practicable and, in any event, within statutory time limits (one month). This may be extended to two months if the request or accessing the data is complex, however the individual will be informed of this within the one month timescale.

There will be no charge for providing access to information, unless the request is manifestly unfounded, excessive or repetitive. A charge may be made for providing further copies of information to which the data subject has already been given access. The charge will be based on actual cost of providing the information and the individual will be advised in advance in writing.

Certain data is exempt from the right of access under the Act; this may include information which identifies other individuals or information which is subject to legal professional privilege.

2.5.1 Data Portability

The right to data portability allows individuals to obtain and reuse there personal data for their own purposes across different services. Requests should be made to the DPO. Where the data can be made available in a commonly used machine readable format, the request will be actioned within one month. There is not charge for providing this data.

2.5.2 The Academy's Rights to Refuse a Request

The Academy reserves the right to refuse a request to view or amend data held. This would be rare and only on the following basis :

- Vexatious requests
- Where information held may be required by future legal processes e.g. Child Protection
- The request would lead to inaccurate and misleading information being recorded
- The request has come from an individual who has no rights of access

Where the Academy decides not to adhere to a request it will notify the person who requested of the reason why the request has been refused; their legal rights of appeal or complaint; their legal rights of referral to the ICO.

2.6 Sharing Data

The Academy may receive requests from third parties to disclose personal data it holds about students, their parents or employees. The Privacy Statements will indicate how and when Academies share data with individuals or organisations outside the Trust. The Academy confirms that it will only disclose information if it is included in the Privacy Statement; the individual has given their explicit consent or one of the specific exemptions under the Act applies.

2.7 Automated Decision Making

Individuals have the right to not be subject to a decision based solely on automated processing if it produces a legal effect or similarly significant effect on the individual. It is unlikely that the Academy will make any decisions based purely on automated processing. If automated processing is used for any decision making, the individual will be informed. In most cases the process will involve some human intervention either at the initial decision making point or in an appeal process.

2.8 Record Retention

The Academy will not keep personal data for longer than is necessary for the purpose or purposes for which they were collected and will take all reasonable steps to destroy, or erase from its systems, in a secure manner all data which is no longer required in line with the Academies' Data Asset Maps.

The Academy will dispose of its IT equipment in a manner which will protect data security, in line with the Academies' IT Security Policies.

In certain cases, individuals have the right to obtain the erasure of their personal data where the data is no longer necessary in relation to the purpose it was originally collected/processed and its erasure does not conflict with the Trust's legal responsibilities. We recommend that individuals who wish to have their data erased check the guidance on the ICO website and the Trusts' Record Retention Policy before putting their request in writing to the DPO.

2.9 Data Security

The Academy will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against accidental loss of or damage to, personal data. Academy processes will be in place to ensure the security of personal data about individuals, and that members of staff will only have access to personal data relating to students and their parents, or employees, where it is necessary for them to do so.

All staff will be made aware of this policy and their duties under the Act as detailed in section 3 of this policy.

This policy must be read in conjunction with the Academies' IT Policies.

2.10 Exemptions

Certain data is exempted from the provisions of the Act, including the following:

- The prevention or detection of crime
- The assessment of any tax or duty
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the Academy
- Information which might cause serious harm to the physical or mental health of the student or another individual
- Cases where the disclosure would reveal a child is at risk of abuse
- Information contained in adoption and parental order records
- Information given to a court in proceedings under the Magistrates' Courts (Children and Young Persons) Rules 1992
- Copies of examination scripts; and
- Providing examination marks before they are officially announced

The above are examples only of some of the exemptions under the Act.

Further exemptions may include information which identifies other individuals, information which the Academy reasonably believes is likely to cause damage or distress, or information which is subject to legal professional privilege. The Academy will also treat as confidential any reference given by the Academy for the purpose of education, training or employment, or prospective education, training or employment. The Academy acknowledges that an individual may have the right to access a reference relating to them received by the Academy. However, such a reference will only be disclosed if such disclosure will not identify the source of the reference or where, notwithstanding this, the referee has given their consent or if disclosure is reasonable in all the circumstances.

For further information on exemptions individuals may contact the DPO.

2.11 Privacy Impact Assessments

A Privacy Impact Assessment will be carried out for any new policy or process which involves the processing of personal data.

3 RESPONSIBILITIES AND COMPLIANCE

Those who are involved in the processing of personal data are obliged to comply with this Policy when doing so. Any breach of this Policy may result in disciplinary action. Data breaches carry heavy fines from the ICO, therefore it is essential that the Trust, each organisation and every member of staff are aware of their responsibilities.

3.1 Audit and Risk Committee

Audit and Risk committee will review and approve this policy on an annual basis and recommend to the Trust Board for ratification. They will make the appropriate resources available to support the work of the Data Protection Officer, including any necessary training.

A Trust Governor will sit on the Data Protection Committee.

3.2 The Senior Leadership Team

The Senior Leaders in Academies will support the work of the Data Protection Officer in implementing this policy in their institutions and ensuring the necessary processes and procedures are in place to comply with legislation. A senior member of staff in each Academy will be nominated as the named person for data protection in their organisation.

New staff induction programmes and staff training programmes will include annual updates to Data Protection. Departments will maintain appropriate records relating to the processing of data.

3.3 Data Protection Officer

The Trust has appointed Corinne Walker as Data Protection Officer (DPO), who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the Act. They will report to the Senior Leader stated above. Their responsibilities include:

- Inform and advise the Trust and its employees about their obligations to comply with GDPR and other data protection laws;
- To monitor compliance, train staff and conduct internal audits and Privacy Impact Assessments;
- To be the first point of contact regarding data protection issues;
- To deal with any data breaches and report a breach to the ICO if necessary.

The DPO will log Subject Access Requests, requests for data rectification or erasure and objections. The log will include details of the request and action taken.

The DPO will ensure that Data Protection Policies and Information are made available via the Trust's website.

3.4 Data Protection Committee

The Data Protection Committee will meet at least once a year and include a Trust Governor, the Data Protection Senior Leader, the Data Protection Officer, nominated data protection lead from each institution and relevant support staff from each organisation, including HR Manager, Network Manager, Academy Business Manager, MIS/Student Services Manager, Finance/Contracts Manager as appropriate.

The role of the committee is to work with the DPO to ensure compliance at all levels, including reviewing data audits, privacy impact assessments and subject access request logs, plus determining training plans and a communication strategy relating to data protection. The Data Protection Committee will report to the Audit and Risk Committee annually.

3.5 Staff Responsibilities

Staff have access to a wide range of personal data about students, their parents and possibly employees, Governors and other third parties. All staff are required to read and understand their legal responsibilities under this policy and GDPR and attend compulsory training as required. Any data security breaches should be referred to the DPO.

Staff have responsibilities under the Act to ensure that data **(including computerised and manual records and images**) is obtained and processed fairly and lawfully in the course of your duties, whether on or off site. Staff should not collect, process, publish or disclose data in any way not described in the appropriate Privacy Statements. They should notify the DPO if they require to collect and process any additional data, this includes introducing new software into their practice. Failure to follow this policy could result in disciplinary action.

Staff need to ensure the security of data, therefore they should:

- only store data on the Academy network which is secure and password protected;
- if personal data does need to be stored on a home PC or personal device it must be encrypted;
- keep IT passwords confidential and do not leave PCs in shared areas logged on when not in use;
- lock PC screens when away from their desk;
- keep student and employee manual records in a secure place, eg locked office or filing cabinets;
- encrypt files containing personal data if they are being emailed to an external email address;
- do not open software storing personal info when your PC is linked to an electronic whiteboard;
- do not leave student and staff personal data where unauthorised people may see it;
- dispose of data carefully, in particular sensitive manual records should be shredded or recycled using red confidential waste bins when no longer required.
- ensure that any personal devices (phones, iPads, etc) that have access to the Academy network or email account have adequate security in terms of encryption or password/passcode protection and that the device automatically locks if inactive for a period of time. It is your responsibility to ensure the security of data or access to the college network on your device.

Information should not be held beyond the life of its purpose; staff only have the right of access to data during their employment at the Trust. On leaving the Trust they should return or dispose of any student/staff files (either manual or computerised) and should delete data held on personal devices.

Staff should be aware that individuals can request access to all information held about them, therefore staff should ensure that records based on opinion are based on fact and worded appropriately.

Staff should make staff/students aware if they are taking photographs of them to be used for Academy publicity or posted on social media.

3.6 External Data Processors/Third Parties

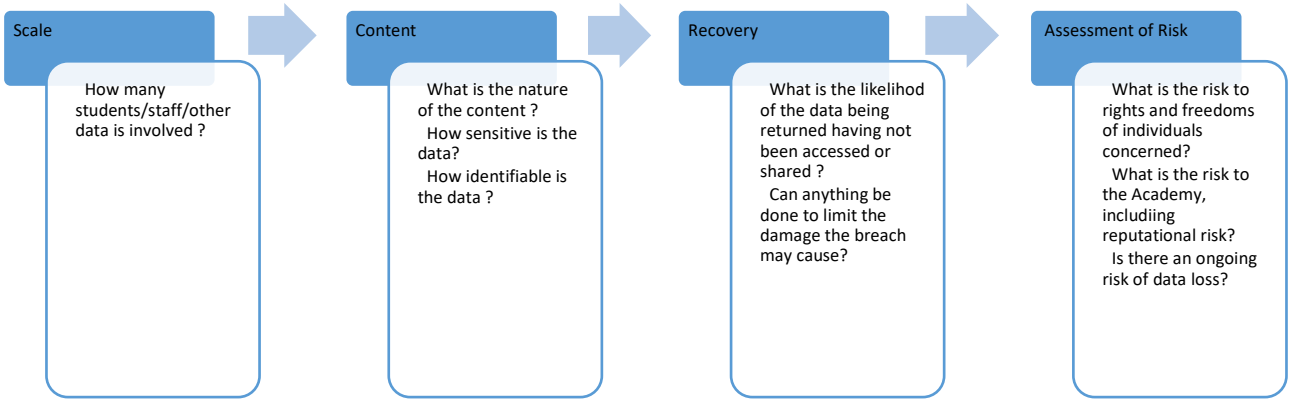
The Academy will have Processing Agreements in place for third parties contracted to process data. There will be a central record of all Processing Agreements in Academy.

3.7 Data Breaches

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Academy takes seriously any data breach and will, through its policy and practice endeavour to minimise the risk of a breach. However, in the rare circumstances surrounding a data breach the Academy must inform the DPO immediately.

The GDPR states that breaches should be referred to the Information Commissioner's Office (ICO) within 72 hours of disclosure of a breach where it is likely to result in a risk to the rights and freedoms of individuals. The individual concerned must be notified where the breach is likely to result in a high risk to the rights and freedoms of individuals.

The DPO will consider the following factors before referring to the ICO :



The SLT link and Board of Trustees will be notified before the DPO refers an incident to the ICO.

4 COMPLAINTS AND APPEALS

If an individual believes that the Academy has not complied with this Policy or acted otherwise than in accordance with the Act, they should notify the DPO in the first instance and/or utilise the Trust Complaints Procedure if appropriate. The Complaints Procedure can be found on the Trust website.

Individuals have the right to file complaints about the processing of their personal data with the relevant data protection authorities if they feel the Academy has not complied with their request. In case of a breach of the applicable legislation on processing of (their) personal data, individuals have the right to claim damages that such a breach may have caused them.