THE PAINSLEY CATHOLIC ACADEMY

The Painsley Catholic Academy

Better Together

Data Protection and Information Security Policy April 2020-2022

Index

GDPR

The General Data Protection Regulation (GDPR) is a piece of EU-wide legislation which will determine how people's personal data is processed and kept safe, and the legal rights individuals have in relation to their own data.

The GDPR lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow "good information handling principles". Guidance on the GDPR is available on the Information Commissioners Office website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Introduction

Painsley Catholic Academy is registered as a data controller with the Information Commissioners Office (ICO) to process personal information to enable us to provide education, training, welfare and educational support services, to administer school property; maintain our own accounts and records, undertake fundraising and to support and manage our employees. We also use CCTV for security and the prevention and detection of crime and a biometric system for sixth form student access to the sixth form building.
https://ico.org.uk/ESDWebPages/Entry/Z3332453

Our MAC is "data rich" and the introduction of electronic storage and transmission of data, alongside paper records has created additional potential for the loss of data. Painsley MAC recognises that loss of personal data can have a damaging effect on individuals which may affect their personal, professional or organisational reputation. It can also bring the MAC into disrepute and may result in disciplinary action and / or criminal prosecution. To safeguard the data processed or held, Painsley MAC is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation.

Our MAC holds personal data on the pupils in our care, and increasingly this data is held digitally and is accessible not only in the schools/colleges but also from remote locations. It is important to stress that this policy applies to all forms of personal data, regardless of whether it is held on paper or in electronic format. For this reason, the security of data is given high priority. Given the personal and sensitive nature of much of the data held in our MAC, it is critical that we adopt these procedures and that information security applies equally and is the responsibility of everyone at all levels.

The purpose of this policy is to provide information and process guidance on how Painsley MAC ensures the confidentiality and integrity of data by managing security, access, amendment and secure destruction.

Policy Statement

Painsley MAC will hold the minimum amount of personal information necessary to enable it to perform its functions and information will be erased once the need to hold it has passed. Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay. All personal data will be fairly obtained in accordance with Painsley MAC's Privacy Notice which is available to all students, staff and Teaching School Alliance members. Data will be lawfully processed in accordance with the principles for processing personal data lawfully and fairly.

1. The lawful basis on which we process data

Public task - (Art. 6 GDPR (1) e https://gdpr-info.eu/art-6-gdpr/

This is because we need to process personal data in order to:

- Carry out a task in the public interest
- Exercise our official authority

Painsley MAC can process data for our schools to run properly, and to fulfil our official functions as set out in law.

Legitimate interests - Article 6(1)(f) https://gdpr-info.eu/art-6-gdpr/

This gives us a lawful basis for processing where:

"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

2. Principles for Processing Personal Data Lawfully and Fairly

Painsley MAC is required to ensure that personal data is:

- **Processed lawfully, fairly and in a transparent manner**
  - Policies relating to GDPR are published on our websites
  - Our Privacy Notice is available on our websites
  - Each school/college in the MAC is registered with the ICO as a data controller
- **Collected for specified, explicit and legitimate purposes**
  - Details of the purposes of processing information and the lawful basis are in the introductory statements of this policy
  - Details of the purposes of processing information can be found on our registration document with the ICO (Appendix 1)

- **Adequate, relevant and limited to what is necessary**
  - The types/classes of information that are processed can be found on our registration document with the ICO. These include:
    - Personal details – see section 3 of this policy
    - Family details
    - Lifestyle and social circumstances
    - Education and employment details
    - Financial details
    - Goods and services
    - Disciplinary and attendance records
    - Vetting checks
    - Visual images, personal appearance and behaviour
  - We may also process sensitive classes (special categories) of information that may include:
    - Physical or mental health details
    - Racial or ethnic origin
    - Religious or other beliefs
    - Trade union membership
    - Sexual life
    - Information about offences and alleged offences
    - Biometric data (thumb print access to sixth form building)
- **Accurate and, where necessary, kept up to date**
  - Staff, parents and Teaching School Alliance members should ensure that the College is informed of any changes to personal details
- **Kept for no longer than is necessary for the purposes for which it was processed**
  - As recommended by the ICO, the College uses the Information and Records Management Society's 'Toolkit for Schools' to determine the retention period for all data.
  - We will only retain the data we collect for as long as it is necessary to satisfy the purpose for which it was collected.
- **Secure from unauthorised or unlawful processing and accidental loss, destruction or damage**
  - Painsley MAC will do everything within its power to ensure the safety and security of any material of a personal or sensitive nature. It is the responsibility of **all** members of the MAC community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:
    - have permission to access that data
    - need to have access to that data.

All transfer of data is subject to risk of loss or contamination. Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data legislation and relevant regulations and guidance from the Local Authority.

3. Personal Data

Painsley MAC and individuals will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances.

We process personal information about pupils/students, and parents/carers including:

- names, addresses, contact details, legal guardianship, contact details, health records
- curricular/academic data e.g. class lists, pupil/student progress records, reports, references
- any other information that might be disclosed by parents/carers e.g. National Insurance Number and parental date of birth for the purpose of applying for free school meals/ pupil premium funding or by other agencies working with families or staff members

We process data relating to those we employ to work at or otherwise engage to work at our College. The purpose of processing this data is to assist in the running of the MAC including to

- enable individuals to be paid
- facilitate safe recruitment
- support the effective performance management of staff
- improve the management of workforce data across the sector
- inform our recruitment and retention policies
- allow better financial modelling and planning
- enable ethnicity and disability monitoring
- support the work of the School Teachers' Review Body

This will include but is not limited to:

- contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics such as ethnic group

- Medical information
- Outcomes of disciplinary procedures

The Teaching School Alliance processes the following data about its members

- Name
- Current school
- Email address
- URN
- Teacher number

We will not share information about staff with third parties without consent unless the law allows us to. We are required by law to pass certain information about staff to specified external bodies such as our local authority and the Department for Education so that they are able to meet their statutory obligations.
Any member of staff wishing to see a copy of information about them that the MAC holds should contact the Data Protection Officer in the first instance.

4. Responsibilities

At Painsley Catholic College the County Council acts as our Data Protection Officer, with Mrs E Baskeyfield being the Data Protection Lead for the school.
Mrs E Baskeyfield, will keep up to date with current legislation and guidance and appoint the Information Asset Owners (IAOs). The Data Protection Lead will ensure that all staff are aware of their data protection obligations and oversee any queries related to the storing or processing of personal data, referring to the County Council when required.
Guidance for Managing Information Risk is available at
http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf

The College will identify Information Asset Owners (IAOs)

IAO	**Information**
Mrs J Hambleton	Medical Forms Care Plans
Mrs L Hill	Personnel Details, FSM
Mrs L Machin	School Draw Results
Mrs C Mycock	Work experience, School reports, Student data tracking
Mrs S Whitworth	Attendance
Mr J Sanders	Personnel – salaries, attendance of staff
Mrs J Stewart-Lilley	HR – recruitment, attendance, discipline etc. of staff

Mr D Bullock/Mrs Harris	Looked after children, child protection
Mrs S Davies	SEN
HOD / Pastoral Leads	Academic progress, child specific information
Mr C Snow	Security of network
Mrs J Brereton	Teaching School Alliance data

The IAOs will manage the information and will understand:

- what information is held and for what purpose
- how information has been amended or added to over time
- who has access to protected data and why

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner. Directors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Director.

5. Registration

The College is registered as a Data Controller on the Data Protection Register held by the Information Commissioner, registration number ZA467250
. https://ico.org.uk/ESDWebPages/Entry/ZA467250

6. Privacy Notice/Fair Processing

Under the "Fair Processing" requirements in the GDPR, the College will inform parents / carers of all students of the type of data they hold on the students, the purposes for which the data is held and the third parties (eg LA, DCSF, QCA, Connexions etc) to whom it may be passed.

This privacy processing notice and the privacy notice supplementary information will be distributed to all parents / people with parental responsibility. Parents / carers of young people who are new to the school will be provided with the privacy notice and the privacy notice supplementary information which details 3rd parties which we are required to share information with.

The privacy notice and the privacy notice supplementary information are also posted on the college web site on the policies page. http://www.painsley.co.uk/parents-students/policies/

7. Consent

As the Painsley MAC has determined that the lawful basis on which we process data is 'Public task', this means that there will be few circumstances when we'll need to seek consent. These will be situations where it is not necessary for us to process the personal data to fulfil our function as a College, such as

- using photographs of pupils/students on our website or other promotional material such as the newsletter
- sending marketing material to prospective students/parents/Teaching Schools Alliance members

For permission such as this, we will request consent from students/parents in a clear and unambiguous manner. *See Appendix 2 for Photography Consent*

The MAC does not need to seek consent in situations that are covered by other lawful bases e.g.

- Sharing child protection concerns and records with the appropriate people or agencies
- Submitting census data to the Department for Education
- Sharing assessment data with other teachers, to allow you to moderate work

Nor for other types of consent, as **the rules only apply to personal data**. Therefore, consent for the following will remain the same e.g. a specific letter with attached consent form.

- School trips
- Showing pupils a specific video in a lesson
- Pupils using specialist equipment e.g. in food technology or art

8. Third Party personal data processing

Any third parties which process data on behalf of Painsley MAC should also meet the GDPR requirements. This means any existing contracts and new contracts will be reviewed to ensure they cover all the required points. This includes providers such as insurers and payroll. These contracts will need to reflect the GDPR requirements.

9. Training & Awareness

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings/ briefings/ Inset training
- Day to day support and guidance from Information Asset Owners

10.Secure Storage of and Access to Data

Paper files are kept in securely locked storage. Only those who have been given authorisation by the Data Protection Lead or the Senior Leadership Team to access those files may do so. The purpose of access may be for filing, retrieval of files to forward to another school or to seek information held on that file. Files should not routinely be removed from the storage area. Where a file is removed for examination it should be returned to its correct position expediently.

The MAC will ensure that ICT systems are set up so that the existence of protected files are hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to sensitive data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system (SIMs).

All users will be given secure user names and strong passwords which must be changed regularly (see the MAC's ICT Security Policy http://www.painsley.co.uk/parents-students/policies/). User names and passwords must never be shared. Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto-lock if not used for five minutes. All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on MAC equipment (this includes computers and portable storage media). Private equipment (i.e. owned by the users) must not be used for the storage of personal data. When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected and
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software (memory sticks will not provide this facility)
- the data must be securely deleted from the device, in line with College policy (below) once it has been transferred or its use is complete

The MAC does not allow data protectively marked as 1 or higher to be stored on removal media such as memory sticks, even if encrypted. The MAC has clear policy and procedures for the automatic backing up, accessing and restoring of all data held on College systems, including off-site backups (see ICT Security Policy). All paper based sensitive material must be held in lockable storage. *See Appendix 4 – Use of technologies and Protective marking*

Painsley MAC recognises that data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. The MAC has 1 month to comply with any request and will not charge for this.

Secure Transfer of Data and Access Out of College

Painsley MAC recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school/college.
- When sensitive or personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should only access it via a secure remote connection to the management information system or learning platform

If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location:

- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event. (nb: to carry encrypted material is illegal in some countries)

Transfer to a new school

If a pupil moves school, the transfer of electronic files will be done via the DfE Secure Access portal. Paper files will be sent via recorded delivery and a receipt is included which must be returned, to confirm it has been received.

11.Subject Access Requests *See Appendix 3 for Subject Access Request form*.

Individuals have the right to access the personal data and supplementary information you hold about them. This right applies to everyone whose personal data your school holds, including staff, governors, volunteers, parents and pupils. This information will be provided free of charge and the MAC has 1 month to comply with this request. The information will be provided in a commonly used electronic format if the request has been made electronically. The Data Protection Officer for the individual school/college will deal with all subject access requests. Individuals may still submit requests to other members of staff. There should be forwarded to the Data Protection Officer. Staff members should know how to identify a request e.g. parents may not use the term 'subject access request' but might ask to see their child's behaviour record. This is personal data so these rules apply.

- On receiving a request, the individual will be contacted via phone to confirm the request was made and the identity of the person making a request will be verified using 'reasonable means'. E.g. two forms of identification may be requested, although this won't always be necessary - for example, staff, governors and pupils will be known to the school, so you could simply ask another staff member to verify their identity.
- In most cases the information will be provided within 1 month, and free of charge. If the request is complex or numerous, the school/college can comply within 3 months, but the individual will be informed of this within 1 month with an explanation about why the extension is necessary
- If the request is made electronically, the information will be provided in a commonly used electronic format

School holidays are counted in the response time; if a request is received in the school holidays, the same time-frame will still apply.

'Unfounded or Excessive' Requests

If the request is unfounded or excessive, the school/college can either:

- Charge a reasonable fee for to comply, based on the administrative cost of providing the information
- Refuse to respond
- Comply within 3 months, rather than the usual deadline of 1 month - the individual will be informed of this within 1 month with an explanation about why the extension is necessary

Usually 'unfounded or excessive' means that the request is repetitive, or asks for further copies of the same information.

Refusing a Request

When a request is refused we will:

- Respond to the individual within 1 month
- Explain why we are refusing the requests
- Tell the individual they have the right to complain to the ICO

12. Disposal of Data

The MAC will comply with the requirements for the safe destruction of personal data when it is no longer required. The disposal of sensitive data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

As recommended by the ICO, the Academy uses the Information and Records Management Society's 'Toolkit for Schools' to determine the retention period for all data. https://irms.org.uk/page/AcademiesToolkit

13. Right to Erasure

Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

When does the right to erasure apply?

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which it was originally collected or processed
- you have to do it to comply with a legal obligation (e.g. following recommended retention periods)

When does the right to erasure not apply?

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation
- for the performance of a task carried out in the public interest or in the exercise of official authority
- for the establishment, exercise or defense of legal claims

For full information about Right to Erasure please see the ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

Appendix 1

Registration with the ICO

ico. Information Commissioner's Office

Data protection register - entry details

Registration number: ZA467250

Date registered: 20 November 2018
Registration expires: 19 November 2020

Payment tier: Tier 1

Data controller: The Painsley Catholic Academy

Address:
Station Road
Cheadle
Stoke-On-Trent
Staffordshire
ST10 1LH

Other names:
Blessed Mother Teresa's, Stafford
Blessed William Howard
Painsley Catholic College
St Anne's, Weeping Cross, Stafford
St Austin's, Stafford
St Dominic's, Stone
St Filumena's, Caverswall
St Giles'
St John's, Great Haywood
St Joseph's
St Mary's, Brewood
St Mary's, Leek
St Patrick's, Stafford
St Thomas'
The Faber

Appendix 2

Photography Consent

Student's name: **Year: 7 (2020)**

May 2020

Dear Parent/Carer

At Painsley Catholic College, we sometimes take photographs of students. We use these photos in the College's prospectus, on our website, in the newsletter and on display boards around school.
We would like your consent to take photos of your child, and use them in the ways described above. If you're not happy for us to do this, that is no problem – we will accommodate your preferences.

Please tick the relevant box(es) below and return this form to school.
I am happy for photos of my child to be used on the school website and in the school prospectus and/or newsletter. ☐
I am happy for photos of my child to be used in internal displays. ☐
I am happy for my child's name to be used in the newsletter to celebrate their achievements. ☐
I am happy for my child's photograph and/or name to be used in the local press to showcase achievements, events etc. ☐
Or
I **do not** want the school to take or use photos of my child. ☐ ***Please ensure your child is aware of this.***
I **do not** want my child's name to appear in the newsletter. ☐

If you change your mind at any time, you can let us know by emailing: office@painsley.staffs.sch.uk, calling the school on 01538 493777, or by visiting the school reception.
If you have any other questions, please get in touch.
Why are we asking for your consent?

To ensure we are meeting GDPR requirements, we need to seek your consent to take and use photos of your child. We really value using photos of students, to be able to showcase what students do in school and show what life at our school is like to others, so we would appreciate you taking the time to give consent again.

Parent/Carer's signature: _____ Date: _____

Appendix 3

Subject Access Request form

Painsley Catholic College
Specialist Science College
Specialist Mathematics and Computing College
Principal: Mr S G Bell, BA (Hons), PGCE, MA, NPQH

Station Road, Cheadle, Stoke-on-Trent, Staffs, ST10 1LH
Telephone: 01538 714944
Facsimile: 01538 714962
Email: office@painsley.staffs.sch.uk
Web: www.painsley.co.uk

DATE:

Re: subject access request

Dear Data Protection Officer,

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

Here is the necessary information:

Name	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* • *Your personnel file* • *Your child's medical records* • *Your child's behavior record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*

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

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

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

Yours sincerely,

Use of technologies and Protective Marking

The following (from Becta) provides a useful guide:

	The Information	**The Technology**	**Notes on Protect Markings (Impact Level)**
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual learner's academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically Colleges will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be learners whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the College may decide not to make this learners record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.