Data Protection Policy

Reviewed and Adopted: September 2020

Next review: November 2021

DATA PROTECTION POLICY

Academy 1 Sports College collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the college. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the college complies with its statutory obligations.

Colleges have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Colleges also have a duty to issue a Fair Processing Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related

legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personaldatashallbeprocessedfairlyandlawfully
2. Personaldatashallbeobtainedonlyforoneormorespecifiedandlawfulpurposes 3. Personaldatashallbeadequate,relevantandnotexcessive

4. Personaldatashallbeaccurateandwherenecessary,keptuptodate

5. Personaldataprocessedforanypurposeshallnotbekeptforlongerthanisnecessaryfort he purpose or those purposes
6. Personaldatashallbeprocessedinaccordancewiththerightsofdatasubjectsunderthe Data Protection Act 1998
7. Personaldatashallbekeptsecurei.e.protectedbyanappropriatedegreeofsecurity
8. PersonaldatashallnotbetransferredtoacountryorterritoryoutsidetheEuropeanEcon omic Area, unless that country or territory ensures an adequate level of data protection.

General Statement

The college is committed to maintaining the above principles at all times. Therefore the college will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and

securely

- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to

  personal information, known as Subject Access Requests

- Ensure our staff are aware of and understand our policies and procedures

Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party
- Staff should note that unauthorised disclosure will usually be a disciplinary matter, and maybe considered gross misconduct in some cases

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- If a copy is kept on a removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe

Rights to Access Information

All staff, parents and other users are entitled to:

- Know what information the College holds and processes about them or their child and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what the College is doing to comply with its obligations under the 1998 Act

This Policy document and the College's Data Protection Code of Practise address in particular the last three points above. To address the first point, the College will, upon request, provide all staff and parents and other relevant users

with a statement regarding the personal data held about them. This will state all the types of data the College holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files.

Subject Consent

In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of employment for staff. This included information about previous criminal convictions as jobs will bring the applicants into contact with children.

The College has a duty under the Children Act 1989 and other enactments to ensure staff are suitable for the job. The College has a duty of care to all staff and students and must therefore make sure employees and those who use College facilities do not pose a threat or danger to other users. The College may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The College will only use this information in the protection of the health and safety of the individual but will need consent to process this data in the event of a medical emergency, for example.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the College is a safe place for everyone, or to operate other College policies, such as the Sick Pay Policy or the Equal Opportunities Policy. Because this information is considered **sensitive** under the 1998 Act, staff (and students where appropriate) will be asked to give their express consent for the College to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

Publication of College Information

Certain items of information relating to College staff will be made available via searchable directories on the public Web site, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the College.

Retention of Data

The College has a duty to retain some staff and student personal data for a period of time following their departure from the College, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the College. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

Complaints

Complaints will be dealt with in accordance with the college's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Managing Director or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact the Managing Director who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk