Wyvern Academy

A company limited by guarantee, registered in England and Wales. No 8123602

Data Protection(GDPR)/CCTV

Review of Policy: November 2021

Members of staff responsible: Deputy Headteacher

Policy History: Ratified

Description of Policy Formation and Consultation Process

People involved: **Deputy Headteacher**
Site Manager
Finance & Resources Committee

Signed by Chair of Trustees: _____

Date: 01.12.21

Date for Review: Autumn 2024

Introduction and Rationale

Wyvern Academy collects and uses personal information about staff, students, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education to its pupils and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations, for example the Pupil Level Annual School Census (PLASC) submitted to the DfES.

Schools 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. Schools 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 General Data Protection Regulations (GDPR) May 2018, 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.

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

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) Processed in a manner that 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."

Article 5(2) requires that:

"The controller shall be responsible for, and be able to demonstrate, compliance with the principles."

General Statement

Wyvern Academy is committed to maintaining the above principles at all times. Therefore the school 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 (see appendix)
- Ensure our staff are aware of and understand our policies and procedures

Complaints

Complaints will be dealt with in accordance with the school'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 Headteacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact Mr Bruce Douglas, Headteacher of Wyvern Academy, 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.org.uk** or telephone 0303 1231113.

CCTV Policy

Background

- The Deputy Headteacher is responsible for ensuring the day to day compliance with the requirements of this Code of Practice.
- CCTV is installed primarily outside the Academy, to the front and rear of the building. There are also three cameras inside the Academy, inside the main entrance, outside the site manager's office and outside the swimming pool entrance.
- The purpose of the CCTV is for the prevention or detection of crime and safety of staff. Its use is registered under Dorset County Council's Data Protection Notification (Registration No Z5874509**)** for this purpose.

Siting of the Equipment

- The equipment is sited so that it only monitors those spaces that are intended to be covered by the equipment; operators will not adjust or manipulate cameras to overlook spaces which are not intended to be covered by the scheme.
- CCTV operators will ensure that all measures are taken to ensure that any possible effects on personal privacy are kept to the absolute minimum whilst allowing the efficient and effective use of CCTV for the purposes of the prevention or detection of crime and safety of staff and public.
- Signs have been placed around the Academy to ensure that staff and the general public are aware that they are entering a zone covered by CCTV. Locations are as follows:
    - Kitchen Door
    - Dining Hall, front and side
    - Front of building – outside green class, finance office and food technology window
    - Back fence – outside Sixth Form flat entrance

Quality of the Images

- The CCTV records visual images only
- Images are captured and held on a hard drive within a PC in the Site Manager's office
- The cameras and equipment are properly maintained and serviced at regular intervals to ensure that the quality of images is preserved
- A maintenance log is kept with the Site Manager in the Wey Valley Academy's site office.
- If the CCTV or recording equipment is damaged, the Site Manager is responsible for contacting the maintenance company to ensure that this is fixed.

Processing of Images

- Unless they are required for evidence, images are only retained for 28 days after which time they are erased by the system
- The dedicated CCTV monitor is located in the site manager's office. There is also remote access available in the Reception office. Access to recorded images is restricted to authorised personnel only consisting of Head, Deputy Head, Finance Director, and Site Manager.
- The images will not be removed from this location at any times unless for evidential purposes. The recording medium will then be sealed and given a unique number
- If the images are required for evidential purposes they are given to or retained by the Site Manager until released to the appropriate authority or until no longer required as evidence, at which time they will be erased
- The Site Manager is responsible for ensuring the following is documented:
    - The date the images were removed
    - The reason the images were removed
    - Incident Crime Number and the Name, number, station and signature of the collecting Police Officer or equivalent details as appropriate
    - The unique number given to the sealed medium
    - All staff are aware of their responsibilities under this Code of Practice

Access to and Disclosures of images to third parties

- Access to recorded images is restricted to the Head, Deputy Head, Finance Director and Site Manager.
- Where the CCTV images are being used for the prevention and detection of crime, then the Academy will only provide access to images to the following:
    - Individuals whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)
    - Police where the images recorded would assist a specific criminal enquiry
    - Prosecution agencies
    - Relevant legal representatives
    - The media, through the police, where it is decided that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident should be taken into account
    - Community safety/anti-social behaviour agencies
- The Deputy Headteacher in conjunction with the Headteacher is responsible for deciding whether to allow requests for access to the images by third parties; this will only be done in very limited circumstances
- The Site Manager will document all requests for access to the medium on which images are recorded. If access or disclosure is denied the reason will be documented

- If access is permitted the date and time at which access was allowed and the person who was allowed access and what they will have access to will be documented by the Site Manager.

Access by Data Subjects

- The Deputy Headteacher in conjunction with the Headteacher will co-ordinate all requests for access to recorded images by a Data Subject.
- The Data Subject will be asked to provide a Subject Access Request (Appendix 1) in writing which includes the following:
    - Sufficient details to locate and retrieve the images requested i.e. date/time/location/description of clothing etc. As the individual will probably be unknown a photograph of the individual can be requested
    - Proof of identity
    - The requisite fee; the maximum fee that can be charged to carry out the searches for images is £10
- A response to a request will need to be provided promptly and in any event within 40 days of receiving the required fee and information
- The Deputy Headteacher in conjunction with the Headteacher will need to determine whether images of third parties can be disclosed. If they cannot be disclosed then the images will be disguised or blurred.

Monitoring compliance with this Code of Practice

- The Deputy Headteacher will undertake a review periodically to ensure the provisions of this Code are being complied with.
- The Site Manager is responsible for ensuring that all staff involved in operating the CCTV system are aware of the following:
    - of the requirements of this guide on the use of CCTV systems
    - that they are dealing with personal information covered by the Data Protection Act 1998 and that individuals have rights under the Act in relation to CCTV systems
    - how to handle requests for access to CCTV images

Appendix – Procedures for responding to subject access requests made under the General Data Protection Regulations 2018

Rights of access to information

There are two distinct rights of access to information held by schools about pupils:

1. Under the GDPR 2018 any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the GDPR 2018.

Actioning a subject access request

1. Requests for information must be made in writing, which includes email, and be addressed to Mr Douglas, Headteacher. If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth/Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. Under GDPR 2018, the school is not permitted to make a charge for the provision of information

5. The response time for subject access requests, once officially received, is 30 days **(not working or school days but calendar days, irrespective of school holiday periods)**

6. The GDPR 2018 exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure**.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 30 day statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought from the Information Commissioner's Office.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Complaints

Complaints about the above procedures should be made to the Chair of the Trustee Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.
Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding these policies/procedures then please contact Mr Douglas, Headteacher.

Further advice and information can be obtained from the Information Commissioner's Office, **www.ico.org.uk** or telephone 0303 1231113.

This policy/procedure is to be read in conjunction with all others that come under the Wyvern Safeguarding family of policies.
These are: Child Protection, Behaviour (including anti-bullying), Staff Code of Conduct, SRE, Intimate Care, Medical, Whistle-Blowing, Health and Safety, E-Safety, Safer Recruitment, Complaints, Allegations Procedures, Attendance (pupils), Data Protection, Looked after Children, Lone Working, Manual Handling, Pool Safety Operating Procedures, and Violence at Work.

As such, reference is made to the key guidance documents: Keeping Children Safe in Education 2018 and Guidance for Safer Working Practice 2015.