GDPR Policy

Date Reviewed: June 2018

Date Policy Approved: Sept 2018

Next Review Date: July 2019

GDPR Policy

Rationale

Wyvern Academy is committed to protecting the rights of all members of the organisation in accordance with the General Data Protection Regulation (May 2018)

We shall ensure that:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
- Personal data shall be adequate, relevant and not excessive
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes (See data retention policy)
- Personal data shall be processed in accordance with the rights of data subjects under GDPR
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data Personal data shall be not be transferred outside of the organization unless the receiving organization ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Wyvern Academy will implement the requirements of the GDPR (2018) and any subsequent amendments or regulations on protecting data, and the academy's controls and procedures will ensure integrity and security of data.

Wyvern Academy will work within the regulations laid out by GDPR and the DPO.

In addition, Wyvern Academy will ensure that:

- A member of the senior management team has overall responsibility for the implementation of GDPR.
- Staff are aware of their responsibilities under GDPR.
- Staff are trained and supported to deal effectively with the requirements of the Regulation, including the need to deal with subject access requests, in whole or in part, in accordance with the Regulation.

The Date Protection Officer has responsibility for maintaining a register of all requests made for information under GDPR that do not fall within the remit of the GDPR with the Information Commissioner's Office, and the action taken on each application.

The Policy and associated procedures and arrangements will be monitored within the context of legislation, including:

- Data Protection
- Computer Misuse

- Human Rights
- Equal Opportunities
- Telecommunications
- Health & Safety

Requests for personal data and charges to personal data

- Requests should be made in writing by letter or email to the Academy, via the DPO.
- Proof of identity (normally a driving licence, passport or utility bill or corporate identification in the case of organisations) will be required before the request can be met.
- The request will be dealt with within the required response time of 30 Calendar days, subject to any extensions as stated within the GDPR.
- If the request is too general the Academy will offer advice and assistance to determine the information required. The Academy does not have the right to ask why information is being sought, but the information can be volunteered to assist the Academy in meeting the request.

Review and appeal

If an applicant is dissatisfied with the handling of a request, they have the right to ask for an internal review. Internal review requests should be submitted no later than 30 working days after the date on which the applicant believes that the academy has failed to comply with the requirement, and should be addressed to The Headteacher:

Mo Wilkinson
Wyvern Academy
Eggleston View
Darlington
DL3 9SH

Email Wilkinson@wyvernacademy.org

If not content with the outcome of the internal review, an applicant has the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Employee Responsibilities

Employees are responsible for:

- Ensuring any information they provide to Wyvern Academy in connection with their employment is accurate and up to date.
- Informing the Academy of any changes to information they have previously provided e.g. changes of address.
- Checking the information that the Academy will send out from time to time giving details of information held and processed. Informing the Academy of any errors or changes.
- If and when employees as part of their responsibilities collect, access and process information for employment records they must comply with the GDPR.

- Line Managers are responsible for ensuring all employees they supervise are aware of their responsibilities under GDPR.

Data Security

Personal information (pupils, employees, commercial or any other information) should be kept in a locked filing cabinet or securely on the learning portal. Information of this nature should not be stored on memory sticks. All employees are responsible for ensuring that:

- Any data which they have is kept secure particularly if taking data off site on laptop computers, tablets or files. If mobile devices are taken off site, they should never be left in a car overnight. A password must be in place for the device. The same precedent applies if personal data is stored on employees own devices.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Ensure any document containing personal data is password protected.
- Personal information is not disclosed either orally or in writing deliberately or accidentally or otherwise to any unauthorised third party.
- No personal information is given to unknown third parties over the telephone. The sharing of personal data is required as detailed elsewhere in the document.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” or “locked” at the end of any session in which they are using personal data.
- If school equipment is to be used by anyone other than the member of staff responsible for it that user must have a separate account set up by the ICT Support Department. The laptop must remain in the user’s possession at all times.
- Equipment is insured whilst in school premises or the registered user’s home. Whilst in transit it is only covered if it is in the possession of the user. If the equipment is in a situation where it is not covered by insurance, users are responsible for organising their own insurance. Any damage not covered by insurance could be charged to the individual.
- If portable data storage devices are used, the MUST carry encryption and be password protected.
- If staff receives work e-mails on their mobile phone as a minimum a 4-digit passcode must be used on the device.

Data Breach

If there is a data breach employees must notify the school DPO immediately. Major data breaches could be reportable to the Information Commissioners Office, within 24 hours. Therefore, it is important that any data breaches are disclosed as a matter of urgency. The headteacher in conjunction with the DPO will review the circumstances of the data breach and decide whether this breach warrants disclosure and any corrective action which may be required.

Employees should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual employee.

Data Sharing

The Academy, Multi-Academy Trust, Local Authority and the Department of Education, hold information on pupils to run the education system. In doing so the Academy has to follow the General Data Protection Regulations 2018. Data help about pupils must be used for specific purposes, allowed by law.

The Academy holds information about staff in its employment records in order to perform key tasks e.g. recruitment, performance monitoring, recording absence and health & safety matters. The Academy must comply with General Data Protection Regulations 2018 to ensure it is collected and used fairly, stored safety and not disclosed to other persons unlawfully.

Pupil Data

The Academy holds information on pupils in order to support their teaching and learning, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the Academy as a whole is doing. This information includes contact details, National Curriculum assessment results, attendance information, and characteristics such as ethnic group, special educational needs and any relevant medical information.

From time to time we are required to pass on some of this data to the Local Authority (LA), to another school, Academy, College to which the pupil is transferring, to the Department of Education, and to the Standards and Testing Agency/Teaching Agency.

The local Authority uses information about pupils to carry out specific functions for which it is responsible, such as the assessment of any special educational needs the pupil may have. As with the Department of Education, it may also use the information to derive statistics to inform decision on (for example) the funding of Academies, and to assess the performance of Academies and set targets for them. The statistics are used in such a way that individual pupils cannot be identified from them.

The Academy must have lawful basis for holding this information.