BWAF

DATA PROTECTION POLICY

DATE: JANUARY 2018

REVIEW DATE: May 2019

Overview

BWAF is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA) or General Data Protection Regulations (GDPR) from 25th May 2018.

Changes to data protection legislation (GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements.

The legal basis for processing data is that it is necessary to carry out these tasks in the public interest.

All staff, governors and Trustees are responsible for data protection.

The Trust Data Protection Officer (DPO) is Darren Rushby
The Data Protection Controller is Jonathan Jackson

The Senior Information Risk Owner (SIRO) and the Information Asset Owner (IAO) for each Academy or the Trust can be identified in the Assets Data Audit Log.

The Trust is committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them.

The requirements of this policy are mandatory for all staff employed by the Trust and any third party contracted to provide services within the Trust.

Policy Statements

The Trust will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the 'Privacy Notice' and lawfully processed in accordance with the "Conditions for Processing".

Personal and Sensitive Data

All data within the Academy's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

Definitions

Personal data: information which relates to an identifiable living individual that is processed as data. Examples would be names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews.

Sensitive personal data: information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences.

Processing data: collecting, using, disclosing, retaining, or disposing of information.

Principles

The principles of the GDPR shall be applied to all data processed:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

Registration

The Trust is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents / Carers / Contacts– the 'Privacy Notice'

In order to comply with the fair processing requirements of the GDPR, the Academy will inform parents / carers of all pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be available on the Trust and Academy websites.

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
- Support and guidance from the Data Protection Officer

Data Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.
Risk and impact assessments shall be conducted in accordance with guidance given by the Information Commissioner's Office (ICO).

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and these organisations shall provide evidence of the competence in the security of shared data.

The Trusts takes its responsibilities in protecting individual's data and any member of staff is found to have caused a data breech they will be subject to The Trust's disciplinary policy.

Photographs and Video:

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in the Trust / Academy only.

Unless prior consent from parents/pupils/staff has been given, the Academy shall not utilise such images for publication or communication to external sources.

Secure Storage of data

The Academy will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected 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.

All users will use strong passwords which must be changed regularly. User 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).

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 Academy 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,
- the device must be password protected
- the device must offer approved virus and malware checking software and
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

The Trust has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

The Trust has clear policy and procedures for the use of Cloud Based Storage Systems (for example DropBox, Microsoft 365, Google apps and Google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the GDPR. The Trust will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the Trust is responsible for the security of any data passed to a 'third party'. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

Data Access Requests (Subject Access Requests):

The Trust recognises that under the GDPR, 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. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. No charge will be applied to process the request. We shall respond to such requests within one month and they should be made in writing to Mr D Rushby or by emailing DPO@BWAF.net

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

Other schools

If a pupil transfers to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

Examination authorities

This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

Health authorities

As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

Police and courts

If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

Social workers and support agencies

In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

Educational division

Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

Secure transfer of data and access out of school

The school 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 restricted or protected 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 (eg family members) when out of school
- When restricted or protected 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 preferably have secure remote access 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 (guidance on this can be obtained from the IT Manager); and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the IT Manager in this event.

Data Disposal:

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance:

The school has identified a qualified source for disposal of IT assets and collections – Enviro electronics www.enviroelectronics.co.uk