new wave education

Grazebrook School

SHACKLEWELL PRIMARY SCHOOL

WOODBERRY DOWN COMMUNITY PRIMARY SCHOOL

High Aspirations

High Standards

High Achievement

Data Protection Policy

2016

This policy is a statement of the aims and principles of the New Wave Federation for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

Introduction

The Federation collects and uses personal information (referred to in the Data Protection Act as personal data) about staff, pupils, parents and other individuals who come into contact with the Federation. This information is gathered in order to enable the provision of education and other associated functions. In addition, the Federation may be required by law to collect, use and share certain information.

The Federation is registered as a Data Controller, with the Information Commissioner's Office (ICO). Details are available on the ICO website.

The Federation issues a Privacy Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other organisations to whom it may be passed on to.

Purpose

This policy sets out how the Federation deals with personal information correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation.

This policy applies to all personal information how it is collected, used, recorded and stored and whether it is held on paper or electronically.

All Federation staff and governors involved with the collection, use, processing or disclosure of personal data will be aware of their duties and responsibilities and will adhere to this policy.

What is Personal Information/ data?

Personal information or data is information which relates to a living individual who can be identified from that data, or from that data in addition to other information available to them. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Data Protection Principles

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

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Commitment

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

- Inform individuals why personal information is being collected.
- Inform individuals when their information is shared, and why and with whom unless the Data Protection Act provides a reason not to do this.
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.

- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- comply with the duty to respond to requests for access to personal information, known as Subject Access Requests.
- Ensure that personal information is not transferred outside the EEA (European Economic Area) without the appropriate safeguards
- Ensure all staff and governors are aware of and understand this policy and procedures.

Status of this Policy
This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the Federation from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

The Data Controller and the Designated Data Controllers
The Federation as a body is the Data Controller under the 1998 Act, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters.
The Federation has three Designated Data Controllers: They are the Executive Headteacher, the Heads of Schools and the Senior Administration Officers.
Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller.

Responsibilities of Staff
All staff are responsible for:
- Checking that any information that they provide to the Federation in connection with their employment is accurate and up to date.
- Informing the Federation of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The Federation cannot be held responsible for any errors unless the staff member has informed the Federation of such changes.

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 may be 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 diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.
- Security software is installed on all computers containing personal data.

- The Federation will ensure that ICT 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.
- All users will be given secure user names and strong passwords which must be changed every six weeks. 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 Federation equipment (this includes computers and portable storage media. Private equipment (i.e. owned by the users) must not be used.
- 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 (many memory sticks/cards and other mobile devices cannot be password protected);
- the device must offer approved virus and malware checking software;
- 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 Rights to Access Information

The Senior Administration Officers will ensure that the above measures are met fully and termly monitoring will be sent to the Executive Headteacher for monitoring. See Appendix 1.

All staff, parents and other users are entitled to:

- Know what information the Federation 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 Federation is doing to comply with its obligations under the 1998 Act.

The Federation 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 Federation 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. Any person who wishes to exercise this right should complete the Subject Access Request Form and submit it to the Designated Data Controller.
The Federation aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

Subject Consent
In many cases, the Federation 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 Federation processing some specified classes of personal data is a condition of acceptance of employment for staff. This includes information about previous criminal convictions. Vacancies will bring the applicants into contact with children. The Federation has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. The Federation has a duty of care to all staff and students and must therefore make sure that employees and those who use Federation facilities do not pose a threat or danger to other users. The Federation 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 Federation 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.

Physical Security
Appropriate building security measures are in place, such as alarms, and deadlocks. Only authorised persons are allowed to log on to the computers in the computer room. Perimeter fencing is secure in all areas of the school and all main entry/exit points are accessed by authorized users only.
Disks, tapes and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, using an electronic Entry Sign system and to wear identification badges whilst in the school.

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 Federation is a safe place for everyone, or to operate other Federation 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 Federation to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

Secure transfer of data and access out of the Federation
The Federation 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.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS)
- 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)

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

Retention of Data
The Federation has a duty to retain some staff and student personal data for a period of time following their departure from the Federation, 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. See Records Management Toolkit Policy Retention Schedule.

Conclusion
Compliance with the 1998 Act is the responsibility of all members of the Federation. 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 federation's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

Appendix 1

Data Controller termly check list

I can confirm that the above measures are in place to ensure that Personal Information of staff is kept securely.

Date ……. **Data Controllers name……..**

Method of Security	Please tick
Data is 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 diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe	
Security software is installed on all computers containing personal data	
All ICT 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	
All users will be given secure user names and strong passwords which must be changed every six weeks. 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 is stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation	
Personal data is only stored on Federation equipment (this includes computers and portable storage media. Private equipment (i.e. owned by the users) must not be used	
Personal data is stored on any portable computer system, USB stick or any other removable media the data is encrypted and password protected	
All storage devices must be password protected (many memory sticks/cards and other mobile devices cannot be password protected)	
All storage devices must offer approved virus and malware checking software	
All data is securely deleted from the device, in line with school policy once it has been transferred or its use is complete Rights to Access Information	

Signed …… Date ……..

Data Controller (SAO)

Signed …… Date ……..

Data Controller Executive Headteacher

ACCESS TO PERSONAL DATA REQUEST

(Subject Access Request – SARS)

DATA PROTECTION ACT 1998 (Section 7)

Enquirer's Surname		**Enquirer's Forenames**	
Enquirer's Address			
Enquirer's Postcode:			
Enquirer's Tel No.			
Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?			**YES / NO**
If NO,			
Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?			**YES / NO**
If YES,			
Name of child or children about whose personal data records you are enquiring:	_____ _____ _____ _____		
Description of Concern / Area of Concern			
Description of Information or Topic(s) Requested (In your own words)			
Additional Information			

Please despatch Reply to: (if different from enquirer's details as stated on this form)

Name Address

Postcode

DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent) _____

Name of "Data Subject" (or Subject's Parent) (PRINTED) _____

Dated _____

Policy reviewed	***March 2016***
Adopted by Governing Body	
Review date	***March 2018***