Codsall Federation of Schools

Data Protection Policy (GDPR)

The CHPB Student Privacy Notice 2018/19 can be found by clicking the link below

http://www.cc-hs.com/privacy/privacy.php

Introduction

Why does the Federation need a Data Protection Policy?

The Governing Body of the federation has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Executive Head Teacher and Governors of the Federation intend to comply fully with the requirements and principles of the Data Protection Act 1998 and the General Data Protection Regulation which came into force May 25th 2018.

All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines. By following the procedure, the federation will fulfil its obligations under the act.

Scope

An essential activity within the federation is the requirement to gather and process information about its staff and pupils in order to operate effectively.
This will be done in accordance with the Data Protection Act 1998 and other government legislation. This includes:

- The Freedom of Information Act 2000;
- GDPR may 2018
- The Human Rights Act 1998;
- Regulatory Investigation Powers Act 2000;

- 1990 Computer Misuse Act;
- Telecommunication Regulations Act1999 (Data Protection & Privacy);
- Crime and Disorder Act 1998.

1. Aims

Our federation aims to ensure that all data collected about staff, students, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 1998. This policy applies to all data, regardless of whether it is in paper or electronic format.

The federation will ensure that the Information Commissioners Office is informed of all its uses of information, and will conduct periodic reviews and update those entries.

The 1998 Act places a strong legal duty on the Data Controller (The Schools) to comply with the Act. To this end, the federation has adopted the policy as specified below. The Schools, acting as custodians of personal data, recognize their moral duty to ensure that it is handled properly and confidentially at all times, irrespective of whether it is held on paper or electronic means. This covers the whole lifecycle, including:

- the obtaining of personal data;
- the storage and security of personal data;
- the use of personal data;
- the disposal/destruction of personal data.

The federation also has a responsibility to ensure that data subjects have appropriate access upon written request to details regarding personal information about them.

2. Legislation and Guidance

This policy meets the requirements of the Data Protection Act 1998, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education. It also takes into account the expected provisions of the General Data Protection Regulation, which is new legislation and came into force in May 2018.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Personal data

Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified

Sensitive personal data

- Contact details
- Racial or ethnic origin
- Political opinions
- Religious beliefs, or beliefs of a similar nature
- Where a person is a member of a trade union
- Physical and mental health
- Sexual orientation
- Whether a person has committed, or is alleged to have committed, an offence
- Criminal convictions

Processing

Obtaining, recording or holding data.

Data subject

The person whose personal data is held or processed.

Data controller

A person or organisation that determines the purposes for which, and the manner in which, personal data is processed.

Data processor

A person, other than an employee of the data controller, who processes the data on behalf of the data controller.

4. The Data Controller & Data Processor

The schools process personal information relating to pupils, staff and visitors, and, therefore, is a data controller. Each school delegates the responsibility of data controller to the Executive Head Teacher. The schools are registered as a data controller with the Information Commissioner's Office and renews this registration.

Our Data Protection Officer Staffordshire County Council.

5. Data Protection Principles

The Data Protection Act 1998 is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully,
- Personal data shall be obtained only for one or more specified and lawful purposes,
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed,
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
- 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 not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

6. Data Integrity

The federation undertakes to ensure data integrity by the following methods:

Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs a School of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be available they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the Schools will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

Examples of data would be pupil information on address, family details, free school meals etc., and school staff personnel details.

The Data Protection Officer will decide how long this information is kept and controlled for following Staffordshire County Council procedures and recommendations.

Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the schools to ensure that obsolete data are properly erased. (This is linked to the DfE Retention Schedule of Records Management and advised by Staffordshire CC).

7. Authorized Disclosures

The federation will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the federations authorized officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations;
- pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare;
- pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school;
- staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters;
- unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school. Officers and IT personnel writing on behalf of the LEA are IT liaison/data processing officers, for example in the LEA, are contractually bound not to disclose personal data.
- only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who need to know the information in order to do their work. The school will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

A "legal disclosure" is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

An "illegal disclosure" is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School's registered purposes.

8. Data and Computer Security

The federation undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

Physical Security

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the control room. Printouts and other information areas (Hard drives) are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied. Passwords are used at all times and computers kept locked when not in the room.

Logical Security

Please see ICT policy.

All staff are forced to use encrypted external storage by default, all external media will be banned from September 2018 and replaced by staff accessing data through the schools remote desktop server. External access to the schools network is protected by an adaptive firewall that also monitors logs for multiple failed attempts. Staff and students will be locked out of their accounts after 5 failed attempts.

The schools email and cloud based storage is through Google Apps for Education, Google have their own data protection policy.

Procedural Security

In order to be given authorized access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents must be shredded before disposal.

Storing Personal Information

Overall security policy for data is determined by Data Protection Officer and the Governing Body and monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. The Federations security policy is kept in a safe place at all times.

Any queries or concerns about security of data in the school should in the first instance be referred to Mr. Neil Eveson.

Suspected breach

If I suspect that data has been accessed unlawfully, the Business and Operations Manager will inform the relevant parties immediately and report to the Information Commissioner's Office within 72 hours if necessary. The federation will keep a record of any data breach. All Data breaches must be reported to Mr Dave Buckley within 48 hours to secure the data if possible and to decide if the ICO need to be informed.

9. Roles and Responsibilities

The governing body has overall responsibility for ensuring that the federation complies with its obligations under the Data Protection Act 1998.

Day-to-day responsibilities rest with the Business & Finance Manager as well as the appointed Data Protection Officer. The Data Controller will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

10. Privacy/Fair Processing Notice

10.1 Students and Parents

We hold personal data about students to support teaching and learning, to provide pastoral care and to assess how the schools are performing. We may also receive data about students from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information
- Details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected. We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so.

We are required, by law, to pass certain information about pupils to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices- transparency-and-control/

** 10.2 Staff*

We process data relating to those we employ to work at, or otherwise engage to work at, our schools. The purpose of processing this data is to assist in the running of each school, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected. We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact the Business and Operations Manager.

11. Subject Access Requests

Under the Data Protection Act 1998, students have a right to request access to information the school holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter, email or fax. Requests should include:

- The students name
- A correspondence address
- A contact number and email address
- Details about the information requested

The schools will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

Subject access requests for all or part of the student's educational record will be provided within 15 school days. The school will charge a maximum of £5 for all materials under 50 pages and £10 for all materials 50 pages or over.

If a subject access request does not relate to the educational record, we will respond within 40 calendar days. The maximum charge that will apply is £10.00.

12. Data Access Requests

Requests for access must be made in writing. Pupils, parents or staff may ask for a Data Subject Access form, available from the Schools Office. Completed forms should be submitted to Mr Neil Eveson. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Pupil Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided. Note: In the case of any written request from a parent

regarding their own child's record, access to the record will be provided within 15 school dates in accordance with the current Education (Pupil Information) Regulations.

Parents have the right of access to their child's educational record, free of charge, within 15 school days of a request.

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights. For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 13 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may be granted without the express permission of the pupil.

12.1 Other Schools

If a student transfers from the federation 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.

12.2 Examination authorities

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

12.3 Health Authorities

As obliged under health legislation, the schools 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.

12.4 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.

12.5 Social Workers and Support Agencies

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

9126 DfE and County

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.

12.7 Right to be Forgotten

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

13. Storage of Records & Data Security

13.1 Storage of Records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key and/or encryption password protection when not in use;
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access;
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals;
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment.

13.2 Disposal of Records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.

For example, we will shred or incinerate paper-based records, and override electronic files. We also use an outside company to safely dispose of electronic records using industry standard shredding.

13.3 Photographs and Video

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

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

It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

14. Training

Our staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary.

Any employee deliberately acting outside of the recognized responsibilities may be subject to the council's disciplinary procedures, including dismissal where appropriate, and possible legal action.

15. The General Data Protection Regulation

We acknowledge that the law has changed on the rights of data subjects and that the General Data Protection Regulation has come into force in May 2018.

The links to all stakeholders we share or obtain data from are listed on our website.

16. Monitoring arrangements

The Federation Business and Operations Manager is responsible for monitoring and reviewing this policy. The Business and Operations Manager along with the Data Protection Officer checks that the school complies with this policy by, among other things, reviewing school records annually.

This document will be reviewed when the General Data Protection Regulation comes into force, and then every 2 years.

At every review, the policy will be shared with the governing board.

17. Links with other policies

This data protection policy and privacy notice is linked to the freedom of information publication scheme.

18. Information Commissioners Office

This is the external regulator for Data Protection. The UK's independent body to uphold information rights.

Date of Approval by Governing Body:

_____

Signed by Federation Chair of Governors:

_____

Review date:

May 2020

_____

Person(s) Responsible for Day to Day Management:

Data Protection Officer, Senior Network Manager

_____

Person Responsible for Review
Business and Operations Manager

Review Officer - Mr N Eveson
Review Date - May 2019

Review Officer - Mr N Eveson
Review Date - May 2019