Ysgol Greenfield School

"Opening doors to the future"

CYNGOR BWRDEISTREF SIROL MERTHYR TUDFIL

MERTHYR TYDFIL COUNTY BOROUGH COUNCIL

GREENFIELD SCHOOL

DATA PROTECTION POLICY

Wayne Murphy, Head Teacher.
Rachel Faulkner, Deputy Head - Standards
Carol Conway, Deputy Head - Wellbeing
Gwyn Daniels - Assistant Head

' Opening Doors To The Future '

' Agor drysau i'r dyfodol'

Original Completion Date	**Author**
November 2015	Kira John, Teacher

MONOTORING THE POLICY

This policy will be reviewed bi-annually unless change of circumstances or legislation requires it to be amended earlier.

Signed: …….. Date: ……..

Head teacher

Signed: …….. Date: ……..

Chair of Governors

Review Date **Author**

Our Vision

'To open doors to the future'

Our Mission Statement

That children, staff, parents, carers and all stakeholders work actively in partnership to enable all pupils to realise and reach their full potential.

Aims

- For pupils to operate as independent learners and thinkers
- To inspire a love for learning
- To provide a relevant curriculum for all
- For pupils to value themselves
- To foster a sense of belonging to a community

Our Values

- We create
- We respect each other
- We try our best
- We are a team
- We learn from mistakes
- We celebrate each other's success
- We are polite and considerate
- We produce magic moments

We want every child to be safe and happy in our school. We believe that the key to this is for us all to have self-respect, respect for others and respect for property.

Everyone has the right to:

- Feel safe, cared for and respected.
- Be able to learn to the best of his/her ability and to develop whatever skills he/she possesses.
- Be treated equally irrespective of gender, race, physical characteristics or any other factors.
- Learn and play without disruption.

Everyone is expected to:

- Be responsible for their own behaviour
- Respect the rights of others
- Share our values

Introduction

At Greenfield we collect and use certain types of personal information about staff, pupils, parents and other individuals who come into contact with the school in order provide education and associated functions. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Education Authorities (LEAs), government agencies and other bodies.

This policy is intended to ensure that personal information must be dealt with properly and securely and in accordance with the Data Protection Act 1998 and other related legislation. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

STATUS OF THE POLICY

The head teacher and registered Data Protection Compliance Officer is responsible for ensuring compliance with the Act and with this policy. Any questions or concerns about the operation of this policy should be referred in the first instance to the head teacher.

If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with the head teacher.

DEFINITION OF DATA PROTECTION TERMS

Data Protection Act 1998 (DPA) is the main UK legislation which governs the handling and protection of information relating to living people.

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Anonymised information is information from which no individual can be identified.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. All data subjects have legal rights in relation to their personal data.

Personal data means data relating to a living individual who can be identified from that data and other information in our possession, or is likely to come into our possession. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act.

Data users include all staff whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data processors include any person who processes personal data on behalf of MTCBC. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

Data sharing relates to the disclosure of data from one or more organisations to a third party organisation(s), or the sharing of data between different parts of an organisation. It can take the form of systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and exceptional, one off decisions to share data for any of a range of purposes.

Data sharing agreements/protocols set out a common set of rules to be adopted by the various organisations involved in a data sharing operation.

Notification relates to the Information Commissioner's Offices public register of data controllers. Each registry entry includes the name and address of the data controller and details about the types of personal data they process. Notification is the process by which a data controller's details are added to the register.

Privacy impact assessment (PIA) is a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal data.

DATA PROTECTION PRINCIPLES

All staff that process personal data must comply with the eight enforceable principles of good practice that are set out under Schedule 2 of the DPA. These provide that personal data must be:

(a) Processed fairly and lawfully.

(b) Processed for limited purposes and in an appropriate way.

(c) Adequate, relevant and not excessive for the purpose.

(d) Accurate.

(e) Not kept longer than necessary for the purpose.

(f) Processed in line with data subjects' rights.

(g) Kept secure.

(h) Not transferred to people or organisations situated in countries without adequate protection.

The school is committed to maintain these principles. This means that the school will:

- Tell you what purposes we will use the information for when we collect it.
- If information will be shared we will tell you why, with whom and under what circumstances.
- Check the quality and accuracy of the information we hold.
- Apply our records management policies and procedures to ensure that information is not held longer than necessary.
- Ensure that when information is authorised for disposal it is done appropriately.
- Ensure appropriate security measures to safeguard personal information whether that is held in paper files or on our computer system.
- Share personal information with others when it is necessary and legally appropriate to do so.
- Set out clear procedures for responding to requests for access to personal information.

- Train our staff so that they are aware of our policies and procedures.

FAIR AND LAWFUL PROCESSING

The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is, in this case MTCBC, the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

PROCESSING FOR LIMITED PURPOSES

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

ACCURATE DATA

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

TIMELY PROCESSING

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required.

PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

Data must be processed in line with data subjects' rights. Data subjects have a right to:

(i) Request access to any data held about them by a data controller.

(j) Prevent the processing of their data for direct-marketing purposes.

(k) Ask to have inaccurate data amended.

(l) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

DATA SECURITY

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The officer responsible for compliance with the DPA is the head teacher. The Legal Department is responsible for advising on compliance with the Act.

Any infringement of the Data Protection Act 1998 by staff may expose Greenfield School/ MTCBC and/or the individual to legal action, claims for substantial damages and fines from the Information Commissioner. Any infringement of the Act will be treated seriously by MTCBC and may be considered under disciplinary procedures.

All alleged breaches of the data protection policy shall be notified to the head teacher in the first instance. Where there has been an unauthorised disclosure of personal data the head teacher, along with the Legal Department shall advise on any remedial action.

All serious alleged breaches of the DPA must be referred to the Information Governance Forum, chaired by the Director of Customer Services, where it shall be considered whether the matter should be reported to the Information Commissioner.

The Act requires Greenfield School/MTCBC to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

(m) **Confidentiality** means that only people who are authorised to use the data can access it.

(n) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(o) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

Security procedures include:

(p) Internet AUP Policy

(q) Disposal of ICT Equipment Policy

(r) Email Acceptable Use Policy

(s) Information Backup and Storage Policy

(t) Information/Asset Protection Policy

(u) Internet Acceptable Use Policy

(v) Information Security Policy

(w) Password Policy

(x) Physical Security Policy

(y) Remote Working Policy

(z) Reporting Information Security Events

(aa) Software Compliance Acceptable Use Policy

(bb) Telephone and Facsimile Policy

(cc) Unauthorised Access Policy

EMPLOYEES AND MEMBERS OBLIGATIONS

Employees and Members shall only process personal data that is under the control of, or on behalf of, Greenfield School/MTCBC when there are lawful grounds to do so and where that employee and Member is so authorised by Greenfield School/MTCBC to process that personal data.

Unauthorised processing of personal data by staff includes accessing personal data records for private interest and/or gain, even where access to the record system itself has been granted to the same member for business purposes. Unauthorised processing of personal data also includes disclosure of personal data (including verbal disclosures) to a third party where it is known that the third party is not entitled to receive that data.

Unauthorised processing of personal data is a potential disciplinary matter which will be considered under the relevant disciplinary procedures. Serious breaches of the Act may constitute a criminal offence.

Staff shall exercise personal responsibility in the secure handling of personal data and shall not knowingly or recklessly expose personal data to unauthorised access, disclosure or loss. Where staff are unsure as to appropriate security measures they shall seek advice from their head teacher.

All staff has a responsibility for the proper handling of all personal data; the overall responsibility shall lie with the head teacher.

All staff are data controllers in their own right and are responsible for all personal data that they process.

Where staff are unsure as to any of the provisions of the Act or this policy they shall seek advice from the head teacher or senior management team.

DEALING WITH SUBJECT ACCESS REQUESTS

The following points must be considered.

(dd) A request under the Data Protection Act must be in writing.

(ee) In many cases a letter to the head teacher will be sufficient to identify the information required. If you cannot identify the information required from the initial request you can go back to the applicant to ask for more information.

(ff) The head teacher must be confident of the identity of the individual making the request. This could be done by checking signatures against verified signatures on file or by asking the applicant to produce valid identification, such as a passport or driving license. These checks should be done in addition to proof relationships with the child.

(gg) An individual only has the automatic right to access information about themselves, requests from family members, carers or parents of a minor will have to be considered. The head teacher will have responsibility for whether to comply with a request. Normally the requester will have to prove their relationships with the child and that disclosure is in the child's best interests to the satisfaction of the head teacher. In the event of a child having sufficient capacity to understand the head teacher should discuss the request with the child and take their views into account when making a decision,. There may be a circumstance in which a child can refuse their consent to request.

(hh) The school may charge a statutory fee, currently calculated on a sliding scale, but only if a permanent copy of the information is provided. If a letter is sent out requesting a fee the 40 day calendar day statutory timescale does not begin until the fee is received. It is important though that no request is delayed unnecessarily by the time taken to inform the applicant of a fee.

(ii) The school will make use of exemptions under the Act as appropriate. All files must be reviewed before nay disclosure takes place. Under no circumstances will access be granted immediately or before this review process has taken place.

(jj) Where information has been provided to the school by a third party, for example by the Local Authority, the police, a health care professional or another school, but is held on the school's file it is normal to seek the consent of the third party before disclosing information. This must be done early in the process in order to stay within the 40 day timescale. Even if the third party does not consent or consent is explicitly not give the data may be disclosed. In these cases it may be appropriate to seek additional advice.

(kk) The applicant should be told the data that the school holds, be given a copy of the data, be told the purposes for which it is processed and whether it has been shared with any other party. It is good practise to explain whether data has been withheld and if so why. There may be circumstances where this is not appropriate; the head teacher should at all times consider the welfare of the child. The school should also give details of who to contact in the event of a complaint and the details of Information Commission who can provide independent information.

(ll) Where all data in a document cannot be disclosed a permanent copy should be made and the data obscured or parts of the data can be retyped if this is more sensible. On any event a copy of the full document (before obscuring) and the altered document should be retained together with the reason why the document was altered, This is so, that in the event of a complaint, there is an audit trail of what was done and why.

(mm) Information can be provided by post (registered mail) or on deposit at the school with an officer available to help the applicant. If the latter is used the applicant must have access to a photocopier in case they want a permanent copy of their data. In considering the method of delivery the views of the applicant should be taken into account. Any codes, technical terms or abbreviations should be explained. Any data which is difficult to read or illegible should be retyped.

(nn) Schools should monitor the number of request received and document whether they are dealt with within the 40 day calendar statutory timescale.

PROVIDING INFORMATION OVER THE TELEPHONE

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by the school. In particular they should:

(oo) Check the caller's identity to make sure that information is only given to a person who is entitled to it.

(pp) Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

(qq) Refer the matter to their head teacher for assistance in difficult situations. No-one should be bullied into disclosing personal information.

PERSONAL DATA STORED IN COOKIES

Where the data contained in cookies can be linked to a name, a postal address or even an e-mail address, that information will amount to personal data and be subject to the DPA.

COMPLAINTS

Complaints about the operation of these procedures should be made to the Governing body who will decide if it is appropriate for the complaint to be dealt with under the complaints procedure. (See policy) Complaints which are not dealt with under the schools complaint procedure should be forwarded in writing to the Information Commissioner. It is likely that complaints about personal issues, due process and timeliness will be dealt with by the Governing body; complaints that involve consideration of personal or sensitive data should be referred to the head teacher/governing body/ information commissioner.

MONITORING AND REVIEW OF THE POLICY

This policy will be monitored by the head teacher and Local Authority. The policy is based on legislation and will be kept under review in accordance with legislative requirements and with particular reference to changes in legislation.

Feedback relating to this policy can be made by telephone or via email to the Information Security Officer, 01685 727444 or information.security@merthyr.gov.uk .