Data Protection Policy

Person responsible: Chris Wilson
Date reviewed: May 2019, May 2020, May 2021
Date of next review: May 2022
Governor's Signature: David Bishop

School's Named Data Controller – Head Teacher

Schools Named Data Protection Officer (DPO) – Deputy Head teacher

1 The school will comply with:

1.1 The terms of the 1998 Data Protection Act, and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful.

1.2 Birmingham City Council's Children, Young People and Families Directorate advice and guidance.

1.3 Information and guidance displayed on the Information Commissioner's website.

1.4 The School will follow the 8 Principles of the Data Protection Act;

i. Data must be processed fairly and lawfully.

ii. Personal data shall be obtained only for one or more specific and lawful purposes.

iii. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.

iv. Personal data shall be accurate and where necessary kept up to date.

v. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.

vi. Personal data shall be processed in line with individual's rights under the 1998 Data Protection Act.

vii. 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.

viii. Personal data shall not be transferred to a country outside the European Economic Area, unless that country or territory without an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2 This policy should be used in conjunction with the school's Internet Usage Policy, Retention Policy, Confidentiality Policy, ICT Policy, ESafety Policy, Disciplinary Policy, Grievance Policy and Whistle Blowing Policy.

2.1 The School will have a Disaster Recovery Plan in place.

3 Data Gathering

3.1 All personal data relating to staff, pupils or other people with whom we have contact, whether held on computer or in paper files, are covered by the Act.

3.2 Only relevant personal data may be collected and the person from whom it is collected should be informed of the data's intended use and any possible disclosures of the information that may be made.

3.3 School uses CCTV around its site.

3.4 Cameras will not be set up covertly within School premises.

4 Data Storage

4.1 Personal data will be stored in a secure and safe manner.

4.2 Electronic data will be protected by standard password and firewall systems operated by the school.

4.3 Computer workstations in administrative areas will be positioned so that they are not visible to casual observers waiting either in the office or at the reception hatch.

4.4 Manual data will be stored where it not accessible to anyone who does not have a legitimate reason to view or process that data.

4.5 Particular attention will be paid to the need for security of sensitive personal data; paper files will be stored in lockable cabinets.

4.6 Personal data held on pupils includes contact details, assessment/examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information and photographs.

4.7 Pupil data is used in order to support the education of the pupils, to monitor and report their progress and to provide appropriate pastoral care.

4.8 The School will regularly review the records held to ensure that information is not held longer than is necessary.

4.9 The School will ensure that when information is authorised for disposal it is done appropriately.

4.10 The School will endeavour to remove all photographs of leavers within 2 years.

4.11 the school uses CCTV around its site,

4.12 the school's CCTV use complies with the ICO's code of practice https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

4.13 while permission is not being sought from individuals who are being recorded, the cameras are visible and well signposted,

4.14 the school staff member to be contacted about CCTV is the ICT Operations Manager, Site Manger and/or Head teacher

5 Data Checking

5.1 The school will issue regular reminders to staff and parents to ensure that personal data held is up-to-date and accurate.

5.2 Any errors discovered would be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

6 Data Disclosures

6.1 Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.

6.2 When requests to disclose personal data are received by telephone it is the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.

6.3 If a personal request is made for personal data to be disclosed it is again the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.

6.4 Requests from parents or children for printed lists of the names of children in particular classes, which are frequently sought at Christmas, should be politely refused as permission would be needed from all the data subjects contained in the list. (Note: A suggestion that the child makes a list of names when all the pupils are present in class will resolve the problem.)

6.5 Personal data will not be used in newsletters, websites or other media without the consent of the data subject.

6.6 Routine consent issues will be incorporated into the school's pupil data gathering sheets, to avoid the need for frequent, similar requests for consent being made by the school.

6.7 Personal data will only be disclosed to Police Officers if they are able to supply a WA170 form which notifies of a specific, legitimate need to have access to specific personal data. This form is the agreed procedure between Birmingham City Council and West Midlands Police.

6.8 A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

7. Staff

7.1 The School has a legal duty to ensure staff understand Data Protection and have undertaken training.

7.2 The School will NOT disclose;

i. References received from other employers if disclosure would impart information about another individual. (unless that individual consents.

ii. Documents that would prejudice an employer's business. (ie information regarding redundancies or mergers)

iii. Documents that would give away an employer's negotiating position. (ie regarding salaries)

iv. Documents that are relevant to legal proceedings in relation to legal rights.

v. Documents that might compromise national security or hamper the detection of crime.

7.3 The School's ICT Department will intermittently check staff emails as part of audit or in the event of an investigation; this links in with the School's Disciplinary Policy.

7.4 The School has a legal duty to provide certain organisations with information ie DWP, CSA; the School will inform the staff member that information is being shared with the organisation.

7.5 During recruitment the School will undertake Social Media searches however, this will not influence the decision as to whether someone is offered employment.

8 Governors

8.1 All Governors should receive Data Protection training.

8.2 Governors will agree access levels within School regarding information.

9 Visitors

9.1 All visitors on the School premises should adhere to the School's Conduct for visitors' guidance;

i. ICT usage – no mobile phones used by visitors in public areas whilst on site.

ii. No smart/iwatches used by visitors in public areas on site.

iii. Visitors cannot use their own memory stick; School will transfer data onto a School memory for their use.

iv. No video recordings should be made by visitors whilst on site.

vi. No recording equipment whatsoever should be used by visitors to record voice or video footage.

10 Subject Access Requests

a. If the school receives a written request from a data subject to see any or all personal data which the school holds about them this should be treated as a Subject Access Request and the school will work towards one working calendar month but this would be extended if in the holiday period (reduced staffing).

b. The data subject should be aware where the request is manifestly unfounded or excessive then a reasonable fee for the administrative costs of complying with the request will be charged, in line with guidance from the ICO.

c. Informal requests to view or have copies or personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the school will comply with its duty to respond within the one working calendar month time limit but this would be longer if in the holiday period.

11 This policy will be included in the ***Staff Handbook***.

12 Data Protection statements will be included in the school prospectus and on any forms that are used to collect personal data.