HORBURY BRIDGE CE J&I ACADEMY

DATA PROTECTION POLICY AND PROCEDURE

Value Statement

The Academy has a duty of care to all its children and staff and this includes how it handles and controls access to the sensitive and personal information and data which it holds.
The academy is committed to maintaining the rights of individual's privacy and personal information of individuals connected with the academy through upholding the eight principles of data protection.

LEGISLATION

The Data Protection Act 1998 is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data. It balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to have respect for the privacy of their personal details.

AIMS

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act. 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.

Under the Data Protection Act 1998 all schools processing personal data must comply with the eight enforceable principles of good practice that. data must be:

- processed fairly and lawfully
- obtained and processed for limited purposes which are specific and lawful
- adequate, relevant and not excessive in relation to the purpose for which it is being processed
- accurate and where necessary kept up to date
- not kept longer than necessary for the purpose for which it was collected
- processed in accordance with the data subject's rights under the 1998 Data Protection Act.
- Secure and protected against unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Not transferred to other countries without adequate protection for the rights and freedoms of data subjects in relation to the processing of personal data.

DEFINITIONS

Personal data

Data which relates to a living individual who can be identified from those data or from those data and other information which is in the possession of, or is likely to come into the possession of, the **data controller.**

Data controller

A person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal data are, or are to be, processed.

Processing

Obtaining, recording or holding the data or carrying out any operation or set of operations on the data. It includes organising, adapting and amending the data, retrieval, consultation and use of the data, disclosing and erasure or destruction of the data. It is difficult to envisage any activity involving data which does not amount to processing.

Data processor

Any person - other than an employee of the data controller - who processes data on behalf of the data controller

Personal information

Any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

CURRENT POLICY

The Academy collects and uses personal information about staff, children, parents and other individuals who come into contact with the school including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of data used by the academy. This information is gathered in order to provide education and other associated functions. In addition, there are some legal requirements to collect and use certain types of information to ensure that the academy complies with its statutory obligations.

In compliance with legislation, the Academy is registered and named as the 'Data Controller', with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are available in a public register on the ICO's website.
http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

The Academy will ensure that it follows the principles of Data Protection Act 1998 and so will:

- Inform Data Subjects why we need their personal information, how we will use it and with whom it may be shared. This is known as a Privacy Notice (See Appendix 1). This will be available for children via the Academy website and in hard copy by request. All staff will be made aware of the notice through their appointment and induction process.
- Check the quality and accuracy of the information held. If a data subject informs the school of a change of circumstances their record will be updated as soon as possible. Information received from a third party will be recorded as such. Where a data subject challenges the accuracy of their data and it cannot be updated immediately, or where the new information needs to be checked for accuracy and validity, a record will be made indicating the nature of the dispute or delay.
- Apply record management policies and procedures to ensure that information is not held longer than is necessary (See weblinks for record management guidance) http://www.irms.org.uk/images/resources/infoguides/records_management_toolkit_for_schools_version_4_may_2012.pdf http://www.businesslink.gov.uk/bdotg/action/detail?itemId=1074450470&type=RESOURCES
- Ensure that when information is authorised for disposal it is done appropriately eg by shredding or deleting from the server
- Ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system.
- Only 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 known as subject access in the Data Protection Act **(**See Appendix 2)
- Train all staff so that they are aware of their responsibilities and of the schools relevant policies and procedures (See Appendix 3 for staff guidance on electronic data security (Becta 2009)

RESPONSIBILITIES

All staff are responsible for:

- Checking that any information that they provide to the Academy in connection with their employment is accurate and up to date.
- Informing the Acadmey of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The Academy cannot be held responsible for any errors unless the staff member has informed the Academy of such changes.
- Handling all personal data (eg – pupil attainment data) securely with reference to this policy.

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.

Personal information should:

- Be kept in the Admin or Headteacher's office in locked cupboards. The office doors are lockable when staff are not in them.or;
- If it is computerised, be 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 usb memory key or other removable storage media, that media must itself be password protected and/or kept in a filing cabinet, drawer, or safe.
- Rarely be taken off site. If necessary (e.g. for child protection conference) then, the member of staff is responsible for the security of that information at all times.
- Be transferred to new schools or other authorised receivers either electronically, when directed, or by hand, or post in sealed envelopes, clearly addressed and marked confidential.
- No personal data is to be left on desks or computer screens when staff are not in the office.

RETENTION OF DATA

The School has a duty to retain some staff and pupil personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time.

DISPUTES AND COMPLAINTS

The Academy will try to resolve issues informally and amicably with the individual but if this is not possible any disputes will be referred to the Governing Body.
Complaints relating to information handling will be handled may be referred to the Information Commissioner (the statutory regulator).

This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act 1998.

APPENDIX 1

PRIVACY NOTICE-DATA PROTECTION ACT 1998

We, Horbury Bridge CE J&I Academy, are a data controller for the purposes of the Data Protection Act.. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well your school is doing.

This information includes your contact details, national curriculum assessment results, attendance information[1] and personal characteristics such as your ethnic group, any special educational needs and relevant medical information.

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some information about you to the Department for Education (DfE) and, in turn, this will be available for the use(s) of the Local Authority.

If you want to see a copy of the information about you that we hold and/or share, please contact the Headteacher. If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

http://www.wakefield.gov.uk/CouncilAndDemocracy/AccessToInformation/AccessInformation/DataProtection/PrivacyNotices.htm and
http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

- The Data Protection Officer
  County Hall
  Bond Street
  Wakefield
  WF1 2QW
- Public Communications Unit
  Department for Education
  Sanctuary Buildings
  Great Smith Street
  London
  SW1P 3BT
  Website: www.education.gov.uk
  Email http://www.education.gov.uk/help/contactus Telephone:0370 000 2288

[1] Attendance information is not collected as part of the Censuses for the Department for Education for the following children - those aged under 4 years in Maintained schools and those in Alternative Provision and Early Years Settings.

APPENDIX 2

PROCEDURES FOR RESPONDING TO SUBJECT ACCESS REQUESTS MADE UNDER THE DATA PROTECTION ACT 1998

Rights of access to information

There are two distinct rights of access to information held by schools about children.

1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the Data Protection Act 1998.

Actioning a subject access request

Requests for information must be made in writing; which includes email, and be addressed to the Headteacher**.** If the initial request does not clearly identify the information required, then further enquiries will be made.

The identity of the requestor must be established before the disclosure of any information, and checks will also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

The school may make a charge for the provision of information, dependant upon the following:

- Should the information requested contain the educational record then the amount charged will be dependant upon the number of pages provided.
- Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.
- If the information requested is only the educational record, viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

The response time for subject access requests, once officially received, is 40 days **(not working or school days but calendar days, irrespective of school holiday periods)**. However the 40 days will not commence until after receipt of fees or clarification of information sought

The Data Protection Act 1998 allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure**.

Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school.

Before disclosing third party information consent should normally be obtained.

There is still a need to adhere to the 40 day statutory timescale.

Any information which may cause serious harm to the physical or mental health or emotional condition of the child or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

If there are concerns over the disclosure of information then additional advice will be sought.

Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it will be retyped.

Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover.

The views of the applicant will be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail will be used.

Complaints

Complaints about the above procedures should be made to the Chair of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding these policies / procedures then please contact the Headteacher.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone

APPENDIX 3

STAFF GUIDANCE ON ELECTRONIC DATA SECURITY (Becta 2009)

Working online
Do

- Make sure that you follow academy procedures on keeping your computers up to date with the latest security updates. Make sure that you keep any computers that you own up to date. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and anti-spyware). Get advice from the academy's IT support if you need help.
- Only visit websites that are allowed by the filtering within the academy. Remember the academy may monitor and record (log) the websites you visit
- Turn on relevant security warnings in your web browser (for example, the automatic phishing filter available in Internet Explorer and attack and forgery site warnings in Mozilla Firefox.)
- Make sure that you only install software that the IT support has checked and approved
- Be wary of links to websites in emails, especially if the email is unsolicited
- Only download files or programs from sources you trust. If in doubt, talk to the IT support.
- Check the acceptable-use policy for the internet and ensure that you follow it.

Email and messaging
Do

- Report any spam or phishing emails that are not blocked or filtered to the IT support
- Report phishing emails to the organisation they are supposedly from (Phishing is an attempt to obtain your personal information (for example, account details) by sending you an email that appears to be from a trusted source (for example, your bank)
- Take care using the contacts or address book and check the recipient list before sending. This helps to stop email being sent to the wrong address.
- Always use your academy e-mail address for academy related business and contact

Don't

- Click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as passwords, bank details and so on.
- Turn off any email security measures that the academy IT support has put in place or recommended
- E-mail sensitive information such as personal details unless you know it is encrypted/password protected. (Encryption is a way of scrambling information. It helps stop anyone using the information if they do not have an electronic key or password to unscramble it.)Talk to the IT support for advice.
- Try to bypass the academy's security measures to access your email off-site (for example, forwarding email to a personal account)
- Use a personal e-mail address for sending or receiving academy related business
- Reply to chain emails.

Passwords

Do

- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers)
- Make your password easy to remember, but hard to guess
- Choose a password that is quick to type
- Change your password(s) if you think someone may have found out what they are.

Don't

- Share your passwords with anyone else
- Use your work passwords for your own personal online accounts
- Save passwords in web browsers if offered to do so • use your username as a password • use names as passwords
- Email your password or share it in an instant message.

Laptops

Do

- Shut down your laptop using the 'Shut Down' or 'Turn Off' option
- Try to prevent people from watching you enter passwords or view sensitive information
- Turn off and store your laptop securely offsite, at home as well as work
- Use a physical laptop lock if available to prevent theft
- Lock your desktop when leaving your laptop unattended

Don't

- Store remote access tokens with your laptop
- Leave your laptop unattended unless you trust the physical security in place
- Use public wireless hotspots – they are not secure
- Leave your laptop in your car. If this is unavoidable, temporarily lock it out of sight in the boot.
- Let unauthorised people use your laptop
- Use hibernate or standby.

Sending and sharing

Do

- Be aware of who you are allowed to share information with. Check with you're the Headteacher if you are not sure.
- Ask third parties how they will protect sensitive information once it has been passed to them
- Encrypt all removable media (USB pen drives, CDs, portable drives) which contain sensitive personal information, taken outside your organisation or sent by post or courier

Don't

- Send sensitive information by email unless it is encrypted
- Place protective labels on outside envelopes. Use an inner envelope if necessary. This means that people can't tell from the outside that the envelope contains sensitive information.
- Assume that third-party organisations know how your information should be protected.

Working on-site

Do

- Lock sensitive information away when left unattended
- Use a lock for your laptop to help prevent opportunistic theft.

Don’t

- Let strangers or unauthorised people into staff areas
- Position screens where they can be read from outside the room.

Working off-site

Do

- Only take offsite information you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above.
- Wherever possible access data remotely instead of taking it off-site
- Be aware of your location and take appropriate action to reduce the risk of theft
- Make sure you sign out completely from any services you have used
- Try to reduce the risk of people looking at what you are working with