Winterbourne Junior Girls' School

Winterbourne Junior Girls' School DATA PROTECTION AND INFORMATION MANAGEMENT POLICY

April 2015

Review date: April 2017

Winterbourne Junior Girls' School
DATA PROTECTION AND INFORMATION MANAGEMENT POLICY
April 2015

Introduction
The Data Protection Act 1998 (the Act) is the primary legislation in the United Kingdom, which regulates the processing of information/data about living individuals – this is referred to as 'personal data'.
The Information Commissioner's Office (ICO) is the body responsible for enforcing and overseeing the Act.

GENERAL STATEMENT
The Governing Body of the school has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions. We are bound by the Council's Data Protection Policy.
The Headteacher and Governors of this School intend to comply fully with the requirements and principles of the Data Protection Act 1984 and the Data Protection Act 1988. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

WHAT DOES THE ACT SAY?
There are 8 Key Principles that underpin the processing of data, to ensure this is done in accordance with the Act and to protect the interests of the individual.
Under those principles personal data must be:

- Fairly and lawfully processed (obtained, used, stored, disposed of) and must ensure compliance with Schedule 2 or, in the case of sensitive personal data (see below), Schedule 3 of the Act;
- Held and processed for limited and specifically registered purposes;
- Adequate, relevant and not excessive;
- Kept accurate and up to date;
- Kept for no longer than is necessary;
- Processed in line with individual's subject access rights;
- Kept secure against unauthorised access, loss, disclosure or destruction;
- Made available only to countries with adequate data protection measures.

TYPES OF DATA
Data as defined under the Act may include both facts and opinions about individuals. It also includes information regarding the intentions of the data controller (i.e. the school) towards the individual.
There are two types of data under the Act:

- **Personal Data** - data relating to any living individual who can be identified from the data and includes any indication of the intentions of the data controller.
- **Sensitive Personal Data** - data relating to race or ethnic origin, political opinions, religious or other beliefs, trade union membership; health; sexual orientation, criminal proceedings or convictions of an individual.

WHAT DOES THIS MEAN FOR WINTERBOURNE JUNIOR GIRLS?
As schools process personal data we are required to notify the ICO as a Data Controller. Notification is a statutory requirement.
Under the Act's principles, schools can only process data for the purposes set out in the school's notification to the ICO. This means that we ensure that:

- There is someone with specific responsibility for data protection within the school;

- Everyone managing and handling personal data understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal data is appropriately trained to do so;
- Everyone managing and handling personal data is appropriately supervised;
- Anyone wanting to make enquiries about handling personal data, whether a member of staff or a member of the public, knows what to do;
- Methods of handling personal data are regularly assessed and evaluated;
- Performance with handling personal data is regularly assessed and evaluated;
- Data sharing is carried out in compliance with the Act, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

ENQUIRIES
Information about the school's Data Protection Policy is available from the Headteacher. General information about the Data Protection Act can be obtained from the Data Protection Commissioner (Information Line 01625 545 745, website www.dataprotection.gov.uk).

OBTAINING AND PROCESSING
Winterbourne Junior Girls' School undertake to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.
"processing" means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.
"data subject" means an individual who is the subject of personal data or the person to whom the information relates.
"personal data" means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.
"parent" has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child.

REGISTERED PURPOSES
The Data Protection Registration entries for the school are available for inspection, by appointment, at the school office. Explanation of any codes and categories entered is available from the Headteacher who is the person nominated to deal with Data protection issues in the School.
Registered purposes covering the data held at the school are listed on the school's Registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

Data Integrity
The school 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 the 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 provided to data subjects every twelve months so 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 LA solicitor for data protection for advice. The Headteacher will inform the Chair of

Governors of the process. If the problem cannot be resolved at this stage, either side may seek independent arbitration from the information commissioner. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.
If the data subject wishes to complain about the conduct of the Headteacher or any involved staff in processing the subject notice then they should do this in writing to the Chair of Governors c/o the school.

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 School will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. The Headteacher will check relevant records regularly and has the final say on what must be deleted. These decisions will be made on the advice of the borough solicitor for data protection.

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 Headteacher to ensure that obsolete data are properly erased. *See Records Management Policy 2015 and appendix on Retention Guidelines for Schools*

SUBJECT ACCESS
The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the school's policy is that:

- Requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
- Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.
- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be posted to the requesting parent.

PROCESSING SUBJECT ACCESS REQUESTS
Requests for access must be made in writing.
Pupils, parents or staff may ask for a Data Subject Access form (Appendix I), available from the School Office. Completed forms should be submitted to the Headteacher. 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. Student 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 days in accordance with the current Education (Pupil Information) Regulations.

AUTHORISED DISCLOSURES
The School will, in general, only disclose data about individuals with their consent. However there are circumstances under which the School's authorised 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 LA are IT liaison/data processing officers, for example in the LA, 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.

DATA AND INFORMATION SECURITY
Winterbourne Junior Girls recognises that the personal data it holds is valuable and must be managed properly as accidental loss, unlawful destruction or damage may cause distress to individuals concerned.
Winterbourne Junior Girls undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

STAFF AND GOVERNOR RESPONSIBILITY
It is the user's responsibility to ensure that the following points are adhered to at all times.

- Paper based information and electronic equipment should be kept safe, secure and close to hand especially when out of school. Never leave them unattended. Particular care should be taken in public places.
- Staff and governors must not use USB or any other external memory storage devices.
- Where personal information needs to be transported away from school this should be done on secure portable computing devices (i.e. encrypted school laptops/memory sticks or saved on Fronter) and not as paper documents.
- All portable computing devices used for remote working are secure and are encrypted. Personal computers and other devices must be encrypted before use for school business. When transporting paper copies of personal information away from the school you must get permission from the Headteacher and must record what the information is, when you are taking it off site, the reason for doing so and the date when the information was returned.

- Removal of personal paper based information should only be for short periods and should be returned when the user is next in the office. If the user is subsequently off sick and the information not returned then this should be recorded.
- Paper based information should be kept confidential and secure when in transit and transported in a sealed file or envelope. This should indicate where it should be returned to if found.
- When transferring paper based information by car, ensure it is placed in the boot and is kept locked. Do not leave personal information or laptops in vehicles overnight.
- Personal information that is taken home should be stored in a locked drawer.
- Do not discuss confidential or sensitive work matters where you may be overheard by people who should not have access to the information e.g. in communal areas in the workplace or outside work.
- Return papers containing customers personal information to Council offices as soon as possible and file or dispose it securely in confidential waste bins.
- If paper based information or portable computer devices are lost or stolen then the loss must be reported to the user's line manager immediately and the process for reporting lost information must be followed (available in the Information Management section on the intranet).
- Any employee who chooses to undertake work using their own personal IT equipment is not permitted to hold any database, or carry out any processing of personal or sensitive personal data relating to the Council's employees, or customers.
- Personal information should not be emailed to or auto forwarded to a private non-encrypted school email address. Secure email must be used to send personal information outside of the school network.

WHEN IN SCHOOL:

- Filing cabinets and cupboards containing personal information should be kept locked at all times.
- Information on shared drives or electronic document management systems should only be stored in areas with appropriate access permissions, ie, access is restricted to only those who have a need to view it.
- Do not leave documents containing personal information unclaimed on any printer or fax machine.
- Do not leave documents containing personal information on your desk or open in your classroom overnight or if you are away from your desk/class for long periods.
- Portable devices (laptops/iPads) should be secured (eg. a locked drawer/cupboard) particularly when left unattended and/or overnight in school.
- Any user accessing personal information must only use school-owned equipment.
- Personal data should be stored on a school shared drive or Fronter wherever possible and not held on a portable computer device.
- Personal information must only be disposed of in confidential waste bins.
- Personal files must not be sent by normal post.
- Ensure that all postal and email addresses are checked to ensure safe dispatch of information. When sending personal information by post the envelope should clearly state 'Private – Contents for Addressee only'.
- Ensure that when posting / emailing information that only the specific content required by the recipient is sent.
- Ensure that when sending confidential data within the school by email, the 'privacy' option is always used.

REMOTE AND MOBILE WORKING ARRANGEMENTS
Users must ensure that access / authentication passwords and personal identification numbers are kept in a separate location to the portable computer device at all times.
ACCESS CONTROLS
It is essential that access to all personal information is controlled. This can be done through physical controls, such as locking the home office where practical or locking the computer's keyboard.
Alternatively, or in addition, this can be done by password controls or User Login controls. Portable computer devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.
All data on portable computer devices must, where possible, encrypted. If this is not possible, then all personal or sensitive data held on the portable device must be encrypted.
TRAINING AND AWARENESS
Since all school staff and governors are involved in creating, maintaining and using information, it is vital that everyone understands their responsibilities as set out in this policy. Line managers must ensure that staff responsible for handling personal information are appropriately trained and have experience of Information security and that all officers understand the need for compliance with information security.

NOTIFICATION TO THE INFORMATION COMMISSIONER
The Information Commissioner maintains a public register of data controllers. The London Borough of Croydon is registered as such.
The Act requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.
To this end the Data Protection officer will be responsible for notifying and updating the Council's and elected Member's Notification with the Information Commissioner's Office.

CRIMINAL OFFENCES
Both the school and the individuals may be liable for breaches of the Act. Criminal offences carry fines with a current maximum of £500,000 for serious breaches of the Act or on conviction of indictment, an unlimited fine.
If you require any further assistance please contact:
The Data Protection Officer
Democratic and Legal Services
Chief Executive's Office
London Borough of Croydon
Taberner House
Park Lane
CR9 3JS
020 8726 6000

KEY MESSAGES
- Personal information must be kept secure against unauthorised access or loss.
- Users should be aware of the security dangers and risks associated with working away from school and transporting personal information.
- All personal information held on portable computer devices must be encrypted.
- Paper based copies of personal information should only be removed from school where absolutely necessary and following the required controls.
- It is the user's responsibility to use portable computer devices in an acceptable way. This includes not emailing personal or sensitive information to a non-school email address.

APPENDIX I

ACCESS TO PERSONAL DATA REQUEST
DATA PROTECTION ACT 1998 Section 7.

Enquirer's Surname …… Enquirer's Forenames……

Enquirer's Address……
Enquirer's Postcode ……Telephone Number ……..

Are you the person who is the subject of the records you are enquiring about YES / NO (i.e. the "Data Subject")?
If NO,
Do you have parental responsibility for a child who is the "Data Subject" of the YES / NO records you are enquiring about?
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……