Bowdon Preparatory School

# Data Protection Policy

This policy sets out the schools expectations for classroom practice and the responsibilities of different staff in contributing to an outstanding learning environment it should be read in conjunction with the following policies and documents.

| | |
|---|---|
| School's Aims | School Development and Action Plans |
| Inclusion Policy | Positive Behaviour Policy |
| E-Safety | Anti-Bullying Policy |

## CONTENTS



### Introduction

Bowdon Preparatory School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Bowdon Prep School is responsible for, and subject to, laws and regulations that apply to the security and processing of records, data and personal information. The Governing Body and Headmistress of

the school have overall responsibility for ensuring that all records, data and personal information are securely maintained and that their access and use is at all times compliant with the relevant statutory provisions, specifically but not limited to the Data Protection Act 1998. The Governing Body and Headmistress shall ensure that all those employed by or working for the school are aware of these guidelines and their respective duties and responsibilities in respect of the same.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice to all pupils/parents; this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

## Purpose

This policy is intended to ensure that personal information is dealt with correctly 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 collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

## Personal Information

Personal information or data is defined as data which relates to a living individual - who can be identified from that data - or other information held.

## Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

- Personal 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 adequate, relevant and not excessive
- Personal data shall be accurate and where necessary, kept up to date
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
- Personal data shall be kept secure i.e. protected by an appropriate degree of security
- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

## General Statement

The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds

- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access

### Protecting Data

- All school staff and members of the Governing Body are aware of their responsibilities with regard to data protection and trained in data protection laws and regulations.
- Only authorised and trained staff shall in appropriate circumstances be allowed to make external disclosures of personal data.
- All data used within the School by administrative staff and teachers 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 shall 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.

### Data Storage and Security

We look after your personal data by having security that's appropriate for its nature and the harm that might result from a breach of security this shall include but not be limited to:

- Keeping all School buildings and access to them secure.
- Ensuring computer equipment and all physical records are secured in rooms where they are locked away on only accessible by those authorised to access them.
- Ensuring the School's computer systems and/or any computer equipment whether fixed or portable is loaded with the latest security technology such as encryption systems.
- Ensuring that all those having access to the School's computer systems or devices are trained in computer and data security and aware of the importance of maintaining secure passwords and not disclosing or sharing their information for any unauthorised purposes.
- All staff or otherwise authorised persons having access to School records and data shall be fully referenced and checked (including but not limited to CRB checks).
- Communicating regularly with staff and students about the importance of data protection and security.
- Making it a serious disciplinary offence for failing to comply with this or similar policies

### Requests

Ensure our staff are aware of and understand our policies and procedures Complaints. Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

## Contacts

If you have any enquires in relation to this policy, please contact Mr Evans (Bursar) - who will act as the contact point for any subject access requests. Further advice and information is available from the Information Commissioner's Office, www.ico.org.uk or telephone 0303 1231113.

## Policy Review

This policy will be reviewed - and updated in line with legislation if necessary – every two years

| Date of update | (U) Updated (R) Reviewed by | How was updated disseminated | Parents informed | Policy on website |
|---|---|---|---|---|
| April 2016 | HG (U) | Staff meeting | no | no |
| 3/9/16 | HG (U) | Staff briefing | no | no |
| 2016 | NE (R) | Staff email – all staff to familiarise | | no |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Appendix 1

### Access Request

At Bowdon Prep School, procedures for responding to subject access requests made under the Data Protection Act 1998 and Rights of access to information:-

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

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

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

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

**Making a subject access request:-**

Requests for information must be made in writing - which includes email - and be addressed to the headmistress. 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 should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

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

NB - 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. The Headmistress should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. 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, dependent upon the following: Should the information requested contain the educational record then the amount charged will be dependent 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 it will be free, but a charge not exceeding the cost of copying the information can be made by the Headmistress.

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 pupil 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 should 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 should 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 should be taken into account when considering the method of delivery.
If postal systems have to be used then registered/recorded mail must be used.

### Complaints

Complaints about the above procedures should be made to the Chairperson of the Governing Body – Mrs Gillian Healey - who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaints 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.

## Appendix 2
## Information security roles

Overall responsibility for eSafeguarding rests with the headmistress and governing body, there are some key roles which exist in the delivery of the eSafeguarding agenda. It is important that appropriate individuals within schools are identified and that they fully understand their roles and their associated responsibilities in delivering the roles' core objectives.

The **School Bursar** (Mr Evans) is a senior member of staff who is familiar with information risks and the school's response.

He takes on the following roles:
**Senior Information Risk Officer (SIRO)** The school Bursar is the SIRO. As a member of the Senior Leadership Team he has the following responsibilities;

- to own the information risk policy and risk assessments
- to keep a record of all Information Asset Owners (IAOs) (see below)
- to act as an advocate for information risk management

The SIRO is not the Network Manager; the Network Manager implements decisions made by the SIRO.

**Information Asset Owner (IAO)** has responsibility for compiling or working with specific information of a sensitive or personal nature. Their role is to be clear about;

- what information they hold, and for what purposes
- how this information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed of

### Network Manager
ICT and Data Coordinator (Miss Corrigan) is a member of the senior leadership team. She takes on the following role:

She has responsibility for managing the network, monitoring its performance and security and implementing suitable access controls. Many critical elements of eSecurity procedures are the responsibility of technical support staff such as access control (the network), technical security and remote access. The technical support ensures the school network is protected from malicious content and vulnerabilities. The network is accompanied by a full set of documentation for disaster recovery purposes.

Appendix 3

## Teachers Data Security Questionnaire

### Am I fully aware of my responsibilities with regards data security?

This questionnaire is aimed at teachers and support staff, to assess their awareness and knowledge of data security.

| Question | Agree | Disagree | Don't Know |
|---|---|---|---|
| I have read and understood the schools data security policy. | | | |
| I have my own username and password, for my school computer for access to the school network. | | | |
| Nobody else knows my school network username and password. | | | |
| My school network password is alphanumeric (numbers and letters) and has at least one capital letter in it. | | | |
| My school network password is not based on anything personal to me ie DoB, Pets name | | | |
| I know how to lock my school network computer (Ctrl-Alt-Del) when I leave my computer unattended. | | | |
| I have my own login for the School Information Management System. | | | |
| Nobody else knows my School Information Management System login details. | | | |
| I never write down my passwords. | | | |
| I have different passwords for all the systems I access. | | | |
| I know how to change my passwords on all the systems I access. | | | |
| My computer screen is not visible to others when I am viewing sensitive or personal information. | | | |
| I don't leave physical hardcopy (printed) documents containing sensitive or personal information on my desk unattended. | | | |
| I store sensitive personal information on school servers. | | | |
| I don't save sensitive personal information on my computer. | | | |
| I have to use my school network username and password when logging into my school laptop. | | | |
| I attach my school laptop to the school computer network at least once a week for anti-virus and windows updates to be installed. (via network cable or wireless). | | | |
| I connect to the school network over wireless and connectivity is password protected. | | | |
| I don't store sensitive personal information on my laptop. | | | |
| I use my school laptop offsite. | | | |
| I don't allow my friends and family (unauthorised users) to use my school laptop. | | | |
| I do store sensitive information on my laptop, but the device has full disk encryption. | | | |
| I never copy or save files containing sensitive or personal information on unencrypted removable storage devices such as USB sticks/ disks or CD/DVD's. | | | |
| I never send sensitive personal | | | |

Appendix 4

E-Safeguarding Risk Assessment Form

**High Impact:** Public exposure of restricted information leading to embarrassment, system downtime, or data corruption impacting learning & teaching.

**Medium Impact:** Exposure of protected information to a non-authorised third party, leading to outcomes listed above.

**Low Impact:** Internal exposure of information beyond authorised individuals leading to outcomes listed above.

| **e-Security and/or e-Safety issue** (risk assess these plus others identified) | **Threat** (What could happen) | **Impact** [See definitions above] High: Score 3 Medium: Score 2 Low: Score 1 | **Vulnerability** (What is it you do – or not do – that could lead to the threat materialising) | **Likelihood** High(3): next 6 month Medium(2): next 2 yrs Low(1): unlikely in next 2 years | **Total Score** (Impact x Likelihood ; out of 9) | **Action Plan** (Either risk accepted OR actions to be taken to reduce |
|---|---|---|---|---|---|---|
| Information (restricted/protected) taken out of school on laptop, email etc | | | | | | |
| Use of mobile data storage e.g. memory sticks | | | | | | |
| Use of Internet for data transfer and communication | | | | | | |
| Pupil gaining access to restricted or protected information | | | | | | |
| Remote access via school equipment or home computers | | | | | | |
| Back up (storage) | | | | | | |
| Password misuse or poorly managed | | | | | | |
| Viruses and malicious software installs | | | | | | |
| Inadequate staff and pupil training in e-Security and e-Safety | | | | | | |

Appendix 5

SLT Questionnaire

Assessing the schools position on data security

| Question | Agree | Disagree | Don't know |
|---|---|---|---|
| The school has a data security policy and all staff (teaching and support) have signed an Acceptable Use Agreement and are aware of their responsibilities regarding the data security policy. | | | |
| Staff receive annual awareness training and confirm that they are working within the policy. | | | |
| The school has identified a Senior Information Risk Officer (SIRO). | | | |
| The school has identified its information assets and the Information Asset Owners (IAO) understand their individual responsibilities. | | | |
| All staff understand the schools information classification marking scheme. | | | |
| The school has put in place an incident reporting mechanism for information security breaches. | | | |
| All staff have current eCRB clearance. | | | |
| All new staff receive information security awareness training. | | | |
| All new staff are made aware of privacy responsibilities. | | | |
| The school has a current registration with the Information Commissioners Office. | | | |
| The school has a policy for managing its records both physical and electronic. | | | |
| Paper records are destroyed securely or archived when they are no longer needed. | | | |
| The admin and curriculum servers/pc's are backed up daily. | | | |
| Key individuals have been identified to ensure backup media (tapes/ removable storage media) are rotated in accordance with the backup schedule. | | | |
| All old computers/ laptops and servers have data removed prior to being disposed of. | | | |
| Recordings on digital cameras and other peripheral devices are uploaded or deleted from the device after use. | | | |
| No generic user accounts exist for computer access. | | | |
| Passwords for computer access are changed at a regular interval. | | | |
| All access to the schools information management system is reviewed at least annually. | | | |
| All access to the schools information management system is carried out using a personal username and password. (no generic accounts) | | | |
| Admin computer screens are not visible from public areas of the school. | | | |
| All sensitive or personal information carried offsite on laptops and removable media is encrypted. | | | |

## Appendix 6

### Data security guidance

### What is sensitive or personal information?

A lot of information that you have access to within schools will be classed as publicly available. This information is not sensitive or personal and would not cause anyone or the organisation any harm or embarrassment. However if the information includes sensitive or personal details, this information needs to be handled and protected in accordance with the school's data security policy.

Information of this nature can be in physical (printed out) or in electronic format. Information in electronic format can have access controls applied to it, but these logical controls are deemed useless if the end user prints this information out and leaves it on the printer in a public area of the school. This information could be situated within individual word-processing, spreadsheet or database files or entered into the school's information management system or any other centralised system the school may be using.

Listed below are the types of information which can be categorised as being either sensitive or personal.

### Sensitive

Sensitive information covers any information that you might not want to be made publicly available as it could potentially cause embarrassment or damage to reputation.

- Staff absence records
- Staff contract and pay details
- Contact and next of kin details
- Disability and medical issues
- Pupil special educational needs details
- Pupil assessment data and reports
- Pupil in care or child protection register details
- Pupil free school meal eligibility
- Ethnicity
- Sexuality

## Appendix 7

**Suggested guidelines for using Facebook safely**:

Ensure that all your privacy settings are set to 'Friends Only'. Go to your Account Settings and make sure that the Custom Settings are highlighted and that these show that status, photos and posts are set to 'Friends Only'.

Consider what information you have on your info page and your profile picture. Including brief information and an unidentifiable picture, e.g. sunset, will assist in making your profile indistinctive.

If you have professional and social 'friends' on Facebook, using the group list feature will ensure that you can distinguish what type of information you send to particular groups. Make sure that you do not accept pupils (even those that have recently left the school), parent or carers as 'friends'.

Ensure that you do not bring your professional status and educational institute into disrepute. Make sure that you consider what you post about colleagues, pupils or parents. Taking charge of your digital reputation is important, as unprofessional posts or images will lead to disciplinary action and possible failure to gain employment in the future.

Be careful what photographs you include on your profile. Once these are uploaded, they are very difficult to remove and, using image editing software, they can be altered and merged with other more distasteful images.

Be aware of any spam or potential virus risks sent via rogue posts. It is advisable to check with anti-virus firms if you get any suspicious requests or posts.

If you are alerted to any negative or unscrupulous information about yourself, colleagues or your school on Facebook, inform your headteacher. Further advice to help with cyberbullying incidents etc., can be gained from a professional association such as your Trade Union.

## Appendix 8

### Complying with the Data Protection Act

The Information Commissioner's Office (ICO) has published a report on data protection guidance for schools (Adobe PDF, 472KB).

### Your legal obligations

Schools handle and store personal information about pupils, parents or carers, staff, and governors. Under the Data Protection Act 1998, schools are legally obliged to protect this information. Your school must:

- only collect personal information you need for specific purposes
- keep the information secure
- ensure the information is relevant and up to date
- only hold as much information as you need and only for as long as you need it
- let people know what information is held about them and what it is used for
- allow these people to see the information that is held about them
- notify the Information Commissioner's Office that you process personal information.

Find out more about complying with the Data Protection Act from the Information Commissioner's Office.

### Informing parents and carers

Your school must inform all parents and carers that you hold personal information about each pupil and explain how you intend to use this information. Your school needs to send the parent or carer of every pupil a Privacy Notice, also called a Fair Processing Notice. The notice is renewed every year, so you have to send it to parents in the autumn of every school year. Find out more on our page Privacy Notices.

### Allowing individuals to see their information

Pupils, their parents or carers, staff and governors have the right to see the personal information schools hold about them and to correct the information if it is wrong. Under the Data Protection Act, they can send a subject access request to the school. Find out what your legal obligations are on our page Requests for access to personal information.

### Notifying the Information Commissioner's Office

All schools have to notify the Information Commissioner's Office (ICO) that they handle personal information. Notification is statutory and failure to do so is a criminal offence.

There is a notification fee that schools have to pay annually to keep their registration with the ICO up to date. The fee is £500 for schools that directly employ 250 or more staff, and £35 for schools that directly employ fewer than 250 staff. As the majority of school staff are employed directly by East Sussex County Council, most schools may have to pay only the smaller fee. Find out more using the ICO website links below:

Changes to the notification fee structure

Check if your school has already notified the ICO

Notify the ICO for the first time

Renew your notification

## Appendix 9

## Further reference

**Education | ICO**
https://**ico**.org.uk/for-organisations/education/

**Report on the data protection guidance we gave schools in 2012 - ICO**
https://**ico**.org.uk/media/for.../report_dp_**guidance_for_schools**.pdf

**Schools, universities and colleges | ICO**
https://**ico**.org.uk/for-the-public/**schools**/

**Guide to data protection | ICO**
https://**ico**.org.uk/for-organisations/guide-to-**data-protection**/

## Appendix 10

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

Subject's Surname: ……Subject's Forenames: …….....

Subject's Address: ……..…….

……

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 records you are enquiring about?

YES / NO 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) DATA SUBJECT DECLARATION

I request that the School search it's 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 above.

Signature of "Data Subject" (or Subject's Parent): ……..……

Name of "Data Subject" (or Subject's Parent): ……..……

PRINTED) Date: ……