



DATA PROTECTION POLICY FOR STAFF

2019 - 2020

Belvedere British School seeks to comply with its obligations under the UK Data Protection Act 1998 and UAE Law.

If, as an employee of the School, your job involves collecting, using or storing data about current or prospective students, parents or staff, you have a number of legal responsibilities. These responsibilities apply whether the data is held on a computer or kept as a paper-based record, and includes items such as applications for employment, personal details collected for school trips, or staff home telephone number lists, as well as standard student and staff personal files.

Your responsibilities are to:

- collect only data that is relevant and necessary for the purpose;
- use the data only for the purpose specified;
- ensure that the data is accurate and kept up to date;
- ensure that the data is kept securely and not disclosed to unauthorised people;
- ensure that the data is not kept for longer than necessary.

Some particular points you should note

If you are collecting personal data, ensure that the individuals (children or parents) concerned are aware of the purpose for which the data will be used – by including a statement on the form or letter you are sending. If the data is “sensitive” e.g. relating to health, ethnic background etc, ensure that you ask for the individual’s express consent and seek permission from the Principal to collect such data.

Precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. In certain circumstances it is a criminal offence to disclose personal data to unauthorised third parties. You should ensure that:

- any personal data which you hold is kept securely;
- you do not disclose personal information either orally or in writing to any unauthorised person.

Care should be taken to store all forms of paper based records securely and safely.

If information is computerised, it should be:

- password protected, with passwords being regularly changed, so that only authorised people can view or alter confidential data.
- Screens should not be left unattended when personal data is being processed. Care must be taken to ensure that paper-based records, e.g. staff or student files, or computer printouts containing personal data, are not left where they can be accessed by unauthorised staff.
- When paper-based records are no longer required, they should be shredded or bagged and disposed of securely.

Review Date:	July 2019
---------------------	-----------

Next Review Date:	July 2020
--------------------------	-----------

Principal		Date:	
BBS Board of Governors		Date:	