

New End School Policy Statement Data Protection / Security

1. Scope

- 1.1 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. This policy does not seek to re write the whole legislation, rather to familiarise individuals with the key provisions and to demonstrate that New End Primary School has a commitment to them.
- 1.2 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.
- 1.3 This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy may result in disciplinary proceedings.
- 1.4 The School processes a large amount of personal data such as staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection etc. In addition, the school may be required by law to collect and use certain types of information to comply with statutory obligations of the local authority, government agencies or other bodies.
- 1.5 Personal data is any information which relates to a living individual who can be identified from that data either by itself or alongside any other information we hold (for example, name, address, date of birth, National Insurance number, bank account details etc) and it also includes any expression of opinion about that individual and any indication of any intentions we have in respect of that individual. Personal data can also be held visually or as sound recordings (e.g. this includes but is not limited to CCTV recordings, photographs, video clips, smart / mobile phones, tablets, cameras and other portable media devices).

2. School Responsibilities

- 2.1 As per the Data Protection Act 1998 and as corporate body, the School is the Data Controller and the Governors are therefore ultimately responsible for compliance however designated officers will deal with day to day matters.
- 2.2 New End Primary School will ensure that all personal data is accessible only to those who have a valid reason for using it and not disclosed to any unauthorised third parties. Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data should raise the matter with the appropriate designated officer.
- 2.3 The School has 2 designated officers and they are
Karyn Ray – Headteacher
Annamaria Morris – Bursar
- 2.4 In addition the school will put in place appropriate measures for the deletion of personal data. Manual records will be shredded or disposed of as '*confidential waste*', CDs / DVDs / Disks should be cut into pieces, Audio / Video Tapes and (where applicable) Fax rolls should be dismantled / shredded. Hard drives of redundant PCs will be wiped clean before disposal, or, if that is not possible, destroyed physically.
- 2.5 Appropriate contract terms will be put in place with any third parties undertaking this work on the schools behalf.

2.6 The Freedom of Information Act 2000 requires that a log should be kept of the records destroyed and who authorised their destruction.

3. Staff Responsibilities

3.1 All members of staff are responsible for ensuring that:-

3.1.1 Any personal data which they hold is kept securely.

3.1.2 Any information provided to the school in connection with their employment is accurate and up to date including informing of any changes to information which has been provided (for example changes of address) or any errors spotted.

3.1.3 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. (Unauthorised disclosure may result in disciplinary proceedings)

3.1.4 Any personal data held about other people or collected as part of their responsibilities (for example opinions on reports, references, marks, details of personal circumstances) is kept securely.

3.1.5 Personal data that is written, printed or in electronic format held on an unencrypted disk, USB / portable data transfer device or other removable storage media should be kept in a locked filing cabinet, locked drawer, safe or in a lockable room with key-controlled access. Records containing personal data must never be left where unauthorised personnel can read or gain access to them.

3.1.6 Personal data that is computerised should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up.

3.1.7 Computer screens, terminals, CCTV camera screens or any Visual Display Unit (VDU) that shows personal data should be placed so that they are not visible except to authorised staff. PC screens will not be left unattended without a password protected screen saver being used.

3.2 This policy also applies to staff and pupils who process personal data 'off-site' (for example when working at home). Staff are still responsible in such circumstances and additional care must be taken regarding the security of the data. Any personal data, in any format, will not be taken off the school premises without approval of the Headteacher.

3.3 Under the Data Protection Act 1998 any employee may be personally liable in a court of law for unauthorised disclosure of personal data.

3.4 It is also a criminal offence to gain access to unauthorised information on a computer system under the Computer Misuse Act 1990.

Next revision	Annual
To be reviewed	Autumn term 2017