Data Protection Policy

We understand that, according to the Data Protection Act 2018, personal data should:

- Be obtained fairly and lawfully
- Be held for specified and lawful purposes
- Be processed in accordance with the Person's rights under the DPA
- Be adequate, relevant and not excessive in relation to the purpose
- Be kept accurate and up to date
- Not be kept for longer that is necessary for its given purpose
- Be subject to appropriate safeguards against unauthorised use, loss or damage
- No information is shared to any other organisation without the consent of the parent.

Policy on Use of Personal Data

The setting endorses fully the statements and the intent of the Data Protection Act 2018. The Data Protection principles contained in the Act are designed to protect the rights of the individual.

Definitions

Personal Data means data (manual or computer) which relate to a living individual who can be identified from those data (or from data and other information that is in the possession of, or is likely to come into the possession of, the data controller).

Data means information that is being processed automatically or is recorded with the intention that it should be processed automatically. Any manual data that forms part of an "accessible record" is also included in this definition.

Data Controller means a person who determines the way in which any personal data are to be processed.

Every person must be sure that data held on manual and computer files about individuals is:

- Processed fairly and lawfully
- Accurate and up to date
- Used only for defined purposes
- Kept private
- Kept only for as long as it is useful
- Relevant and not excessive

Disclosure

There should be a policy for confirming the identity of any person requesting information about them. This will be specific to the information system in question. For personal information requested by third parties the policy for disclosure will again be system and

service specific. Formulating and implementing these policies will be the responsibility of the service manager.

Any time that information from a file is given to a third party, the person giving the information must be sure that the third party is properly identified, and authorised and registered to receive the data

Before disclosing personal information to a third party it is essential to check why the data is required and to whom that party intends to disclose it. Only disclose personal information when you have checked that the disclosure is compatible with your disclosure policy and the Data Protection principles.

If you are aware of any data held or disclosures made that break the data protection principles you must report this to your supervisor or manager, or to the Data Protection Officer, in order that the breach may be addressed.

Policy on Authority to Access

The Computer Misuse Act 1990 identifies the legal framework for definition of and prosecution for unauthorised use or misuse of computers and computer systems. Whilst the Act is particularly intended to deal with unauthorised accesses from outside the organisations ("hackers"), it deals equally with unauthorised accesses from inside.

It is essential that you, as a computer user, understand the extent of your authority to use and access systems. Computers used for more than one purpose and those connected to the corporate data network provide the potential for access to a large number of systems and to a great deal of personal, private and confidential data.

This policy makes it your responsibility to guard and protect your ability to access systems that you have authority to use. Passwords must not be written down or passed on (other than to your line manager). Computers must not be left logged in when unattended, particularly those in open access offices.

Any employee finding that they have access to systems and data which they are not authorised to use must report this to their supervisor or manager in order for the access to be removed. Any employee with authority to access data that is no longer necessary to their work must ask for the access to be removed. Any employee who knows that unauthorised access is taking place must report this to their supervisor or manager in order for the access to be removed.

Penalties under the Act fall into two main categories:

- Unauthorised access - Anyone gaining access, or attempting to gain access to computer data they are not authorised to see, may face a fine of up to £2,000 or six months in prison, or both.
- Ulterior intent or unauthorised modification - Anyone accessing data with an ulterior motive, or modifying data without authorisation, may be sentenced to up to five years in prison or an unlimited fine, or both.

Data Security Policy

- Make sure your password is changed regularly
- Do not leave your computer accessible when unattended (a password-protected screensaver can be a simple solution)
- Make sure you are authorized to use the systems you need
- Remember to copy data regularly for security and back-up.
- Store important files in your “home folder” on your network file server if you have one – these are backed up regularly by systems administrators.
- Ensure important email files are stored in an archive folder.

Further important points

All parents are informed when registering that their date is stored electronically and in our locked filing cabinet on site.

No information will ever be shared with a third party (e.g. For marketing purposes) upon written request, parents, staff etc. are entitled to see any information we hold on them either manually or digitally.

All information held on parents and children is strictly confidential – staff are trained in this area and know that all information stored on children/parents/staff is highly confidential and must not be released without express permission of the direct person involved.