Glenmere Langmoor Academy Trust

DATA SECURITY POLICY

Keeping Data Secure, Safe and Legal

The Data Protection Act

Personal data is any combination of data items that identifies an individual and gives specific information about them, their families or circumstances. This includes names, contact details, gender, dates of birth, behaviour and assessment records, whether held electronically or on paper. The Data Protection Act 1998 specifies additional data items as “sensitive personal data”; this includes medical records, criminal convictions and ethnic origin. The Act sets out 8 principles concerning personal data.

Personal data must:

- Be processed fairly and lawfully.
- Be processed for specified purposes. Be
- adequate, relevant ant not excessive. Be
- accurate and up-to-date.
- Not be kept for longer than necessary for the specified purpose. Be
- processed in accordance with the rights of data subjects.
- Be protected by appropriate practical and organisational security. Not
- be transported (including electronically) outside the European Economic area without ensuring protection for the data is at least as good as within the EEA.

Parents and staff must be made aware that the information they give us may be recorded, may be shared in order to provide them with care, and may be used to support audit and other work to monitor the quality of care provided.

Keeping records secure

All forms of record that include pupil/staff identifiable information should be kept securely in locked filing cabinets, password protected electronic databases or other form of restricted access storage when not in use. This includes keeping records secure when visiting pupils in their homes. Employees are expected to take appropriate measures to ensure the security of the record at all times.

When sending sensitive information by fax check that the fax machine is sited in a secure room, it is not used by more than one department and there is a

designated person who will collect the fax. Telephone the recipient and advise that confidential information is being sent to them. Confirm the fax number and request a receipt. Ensure that a cover sheet is sent including the name of the recipient and the following wording:

> The information contained in this fax is STRICTLY PRIVATE & CONFIDENTIAL and intended for the named recipient only. If you are not the named recipient you must not copy, distribute or disseminate this information, nor disclose its contents to any person. If you have received this fax in error please notify the sender immediately. Thank you.

When sending sensitive information by post the following procedure should be followed:

> If sending information to a service or department within the Authority use the internal post system.
>
> Where the public post system is required check the name, department and address of the intended recipient. Use a robust envelope. Mark the envelope 'Private & Confidential, to be opened by addressee only'. Ensure that a return address is recorded on the outside of the envelope. If the information is considered to be highly sensitive the item should be sent by recorded delivery

Ensure access to computer equipment is restricted by closing windows and doors when your office is not in use.

Equipment and paper files should not be left on view in any public setting.
As far as is practical, only authorised persons should be admitted to rooms than contain servers or provide access to data.

All school owned ICT equipment including software should be recorded and security marked.

Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons or members of the public.

Lock your computer screen (Ctrl,Alt and Del) if you are leaving your desk.

Any files that contain personal identifiable information should be saved onto a shared network and not the C: Drive.

Any transfers of confidential information should be secure and the method risk assessed. Encrypted software should be used (AVCO).

Users must not make, distribute or use unlicensed software or data on site.

Access should be afforded on a “need to do” basis and the access of leavers removed promptly.

Passwords must not be shared with other members of staff under any circumstances. Passwords must not be written down and/or left on display or be easily accessible. They should be “complex” passwords and should be changed frequently.

It is advisable to password protect any personal files in particular those that contain potentially embarrassing information about an individual or an organisation.

Mobile devices (e.g. laptops, PDA’s, memory sticks, etc) must be encrypted.

If a PC is to be given to another user, personal data should be removed from it. E.g. Access databases concerning pupils and the Free School Meal information.

See also disposal of PCs below.

Legal

The Data Protection Act 1998 should be considered at all times when recording, sharing, deleting or withholding information.

Do not give out sensitive information unless the person is authorised to receive it. Confirm the reason for the request; check the authenticity of the requester (e.g. ring the switchboard of the organisation they are calling from). Record the name, date and time of the disclosure, reason, who authorised it and the recipient’s details in the pupil/staff record.

Ensure sensitive data, both paper and electronic, is disposed of properly. PCs must be disposed of securely either through ‘Complete Wasters’ (www.completewasters.co.uk) or LEAMIS. Reformatting/deleting a hard drive will not necessarily stop somebody from retrieving data. It is therefore imperative to follow guidelines when overwriting data.

Sending information to your PC’s recycle bin does not delete the data as such; it is recoverable if you know how. You could therefore be in breach of the Data Protection Act 1998 especially if you do not empty the recycle bin regularly.

Paper copies should be shredded.

Leicestershire County Council strongly advises that school policy is not to sell obsolete laptops/memory devices to members of staff.

Breaches of Security

In the event of loss or theft of computer equipment, please inform your line manager, the Head Teacher and the Local Authority. If you feel unable to raise any security issues with your Head Teacher or line manager, reference to the school 'Whistle blowing Policy' may help you to raise your concerns.

Examples of Incidents

Loss of computer equipment due to crime or an individual's carelessness.

Loss of computer media e.g. memory sticks.

Accessing any part of a database using someone else's authorisation either fraudulently or by accident.

Finding the doors and/or windows have been broken and forced entry gained to a secure room/building that contains service pupil/staff records.

Finding a computer printout with a header and personal information at a location outside of school premises.

Finding any paper records about a pupil/member of staff or business of the school in any location outside of school premises.

Being able to view records in an employee's car.

Discussing pupil or staff personal information with someone else in an open area where the conversation can be overheard.

A fax being received by the wrong recipient.

You can report security incidents and weaknesses to the following people:

- Your team leader or manager
- Your Head Teacher
- ICT Service Desk on (0116) 3057785
- The information Security Consultant at County Hall on (0116) 3057693

- System Information Manager, Room G8, County Hall on (0116) 3055783

You can make your report by telephone, face to face or by letter – whichever you prefer.

This policy should be read in conjunction with:

E-Safety Policy
Acceptable Use Policy for Pupils