Data Protection Policy
Protecting Schools Data

Policy Statement:

As part of your role at turn IT on, you may have access to school data, especially when working on or accessing Admin machines or Teacher's machines.

School data must be treated in accordance with the same 8 principles of good practice as detailed in below:

1. Processed fairly and lawfully.
2. Processed for limited purposes and in an appropriate way.
3. Adequate, relevant and not excessive for the purpose.
4. Accurate.
5. Not kept longer than necessary for the purpose.
6. Processed in line with data subjects' rights.
7. Secure.
8. Not transferred to people or organisations situated in countries without adequate protection.

Keeping Data:

Any data kept for a particular job must only be kept for the minimum length of time whilst the job is being carried out.

This can apply to all sorts of information that turn IT on employees may access from data accessed by an MIS Consultant to installation work that requires school plans.

Data Security:

In school:

Turn IT On staff must ensure that appropriate security measures are taken against unlawful or unauthorised processing of data, and against the accidental loss of, or damage to, data. When in a school you must not allow anyone access to restricted areas unless you are fully aware of the identification of the person wanting access.

School data:

You should not share school information unless explicitly required for a piece of work that you are undertaking on behalf of the school. You should not retain school information for longer than needed and any information must be stored in a secure place.

Telephone enquiries:

Any member of staff dealing with telephone enquiries should be careful about disclosing any school data held by us.

In particular you should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked
- Refer to HR for assistance in difficult situations. If you feel uncomfortable or concerned then you should ask for support

Backing Up School Data:

- turn IT on Consultants should not back up school data onto a removable media and then remove it from the school site. All such backed up data should be handed over to the Head Teacher or school Administrator.
- Computers, hard drives and servers that are removed from a school site should be taken straight to the Turn IT On Office and stored securely, they should not be taken home.

Disposing of Machines:

Admin machines and servers

As far as possible turn IT on Consultants should not get involved in the disposal of school admin machines or curriculum machines, however the following advice can be given:

- If any admin PC's from the school are to be re-used, then they should be rebuilt and kept within the school network and not be used outside of the school.
- Admin servers (in workgroups) that were used as workstations that are no longer needed should have their hard drives destroyed and not used around school network
- We do not recommend that admin machines containing confidential data should be wiped or recycled.
- Hard drives should be physically destroyed with a screw driver.
- Curriculum machines that do not contain confidential data can be wiped and recycled according to the WEEE directive.

WEEE Directive:

The Waste Electrical and Electronic Equipment Directive (WEEE Directive) aims to minimise the impact of electrical and electronic goods on the environment, by increasing re-use and recycling and reducing the amount of WEEE going to landfill.

The directive states that, before reusing or recycling, data must be wiped:

The use of a software data erasure tool permanently and securely removes data but preserves the integrity of the Hard Disk allowing reuse of hardware.

This statement has been reviewed in March 2018

Next Review Date: January 2019 (or before if applicable).