****

**ICT Security Policy**

The objectives of the Policy, which is intended for all school staff, including Governors, who use or support the school’s ICT systems or data, are to:

* Ensure the protection of confidentiality, integrity and availability of school information and assets.
* Ensure all users are aware of and fully comply with all relevant legislation.
* Ensure all staff understands the need for information and ICT security and their own responsibilities in this respect.

The integrity of the Staffordshire schools’ network depends on the security policy implemented by each connected school. Information covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

The school’s Senior ICT Technician is responsible for the school’s ICT equipment, systems and data with direct control over these assets and their use, including responsibility for access control and protection. The Senior ICT Technician will be the official point of contact for ICT or information security issues.

**Responsibilities:**

* Users of the school’s ICT systems and data must comply with the requirements of the ICT Security Policy
* Users are responsible for notifying the Senior ICT Technician of any suspected or actual breach of ICT security. In the absence of the Senior ICT Technician, users should report any such breach directly to the Director of Business & Finance.
* Users must comply with the requirements of the Data Protection Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984.
* Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.
* Adequate procedures must be established in respect of the ICT security and implications of personnel changes.

**Physical Security:**

* As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.
* Server rooms must be kept locked when unattended.
* Appropriate arrangements must be applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.
* All school owned ICT equipment and software should be recorded and an inventory maintained.
* Uninterruptible Power Supply (UPS) units are recommended for servers and network cabinets.
* Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons.
* Equipment should be sited to avoid environmental damage.
* Do not leave sensitive or personal data on printers, computer monitors or desk whilst away from your desk or computer.
* Do not give out sensitive information unless the recipient is authorised to receive it.
* Do not send sensitive/personal information which may be deemed confidential via e‐mail or post without suitable security measures being applied.
* Ensure sensitive data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks.

**System Security:**

* Users must not make, distribute or use unlicensed software or data.
* Users must not make or send threatening, offensive or harassing messages.
* Users must not create, possess or distribute obscene material.
* Users must ensure they have authorisation for private use of the school’s computer facilities.
* The Senior ICT Technician will determine the level of password control.
* Passwords should be memorised. If passwords must be written down they should be kept in a secure location.
* Passwords should not be revealed to unauthorised persons.
* Passwords should not be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data
* Passwords should be changed at regular intervals; this is enforced by the ICT network at logon.
* Passwords must be changed if it is affected by a suspected or actual breach of security, e.g. when a password may be known by an unauthorised person.
* Regular backups of data, in accordance with the recommended backup strategy, must be maintained.
* Security copies should be regularly tested to ensure they enable data restoration in the event of system failure.
* Security copies should be clearly marked and stored in a fireproof location and/or off site.

**Virus Protection:**

* The Senior ICT Technician will ensure current and up to date anti‐virus software is applied to all fixed school ICT systems.
* Laptop users must ensure they update their virus protection at least weekly, this is done by simply connecting the device to the schools network.
* The Senior ICT Technician will ensure operating systems are updated with critical security patches as soon as these are available.
* Any suspected or actual virus infection must be reported immediately to the Senior ICT Technician.

**Disposal and Repair of Equipment:**

* The Senior ICT Technician must ensure any personal data or software is obliterated from a PC if the recipient organisation is not authorised to receive the data.
* It is important to ensure that any software remaining on a PC being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.
* The Senior ICT Technician must ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed
* The school will ensure that third parties are registered under the Data Protection Act as personnel authorised to see data and such are bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.
* All empty Toner and Ink Cartridges will be disposed in an environmentally friendly manner where possible. As will other ICT consumables such as printer parts and batteries.

**Security Incidents:**

All suspected or actual breaches of the ICT security, including detection of computer viruses, must be reported to the Senior ICT Technician, or Director of Business & Finance in their absence, who should report the incident immediately to Codsall ICT Support/Help Desk, via the Senior ICT Technician.