GP24– ICT Information Security Management

Last Review Date	November 2017	**Next Review Date**	November 2018
Leader of Policy Review	Headteacher		
Associated Policies	ICT Acceptable Use of Electronic Communications, ICT Information Management		

It is the Policy of the School to ensure that:

- Confidential and personal information will be protected against unauthorised access
- Integrity of information will be maintained
- Regulatory and legislative requirements will be met
- Information governance is maintained and tested
- Information security education and training will be available to all staff
- Potential breaches of information security will be reported and investigated

This means for the school that:

- All users of school information systems must be authorised to do so
- Access to systems and data must have appropriate levels of information security
- Authorised users will be in possession of a unique user ID and password which must not be shared under any circumstances
- Business requirements for the availability of information and information systems will be met
- The role and responsibility for managing information security is performed by the Headteacher or designated person who is also responsible for providing advice and guidance on the implementation of this policy
- The Headteacher is directly responsible for implementing the policy and to make all staff aware of their responsibilities under the policy
- It is a responsibility of each employee to adhere to this policy and all relevant supporting guidelines as applicable
- Access/requests by third parties must be carefully considered before allowing access to data

All breaches of this policy must be reported immediately to Flintshire's Lifelong Learning Data Protection Officer or the Principal Learning Officer for ICT. All serious breaches will be reported to the Information Commissioner's Office (ICO) with the assistance of the LLD Data Protection Officer.

Portable Media and Cloud Storage Policy

This Policy applies to all staff users of the school's ICT systems to achieve and maintain appropriate protection of school data. Examples include, but are not limited to:

- Laptops, notebooks, tablet devices, iPods, iPads etc.
- Cloud storage areas
- DVDs, CD ROMs, floppy disks, memory sticks, external hard drives etc.
- Memory cards and other devices that have the capacity to hold electronic information

The Headteacher is responsible for reporting all lost or stolen portable devices or storage media to appropriate LLD officers in compliance with the ***Reporting Information Security Events*** policy.

Personal, confidential or school data should be stored on encrypted devices (laptops, notebooks, USB memory sticks) or on the secure network. Under no circumstances should personal data (as defined by the Data Protection Act) or confidential data be stored on an unencrypted portable device or storage media, or held in cloud storage areas without appropriate levels of protection.

Good practice guidelines are:

- Only copy data that you actually need and where possible anonymise data
- Ensure that your storage facility holds data in an encrypted form
- Mobile devices should not be left unattended at any time. Keep the device securely on your person and if this is not possible then the device must be locked away securely when unattended
- Only transport what is necessary, even information you may not consider to be confidential can be dangerous in the wrong hands
- Report any lost or stolen devices to the Headteacher immediately
- Only store data for as long as necessary and delete from the device as soon as possible

Reporting Information Security Events Policy

All school staff assigned a Flintshire user id (whether employees, contractors or temporary staff and third party users) are required to be aware of and to follow this procedure to ensure information security events and weaknesses are communicated in accordance with Flintshire's LLD Data Protection Breach management plan.

Events are managed using the five-point **Data Protection Breach Management plan**. The LLD Data Protection Officer will visit the school to gather the precise details.

1. *Fundamental Details* – Contacts and incident outline will be recorded immediately the incident is discovered and appropriate officers at FCC will be contacted immediately or as soon as feasible
2. *Containment Recovery* – Develop a Recovery Plan, Incident Response Damage Limitation. This may include immediate searches for lost data, isolating insecure ICT systems etc.
3. *Data Risk Assessment* – Establish what type of information, how sensitive, who is affected (number, consequences), how serious, how substantial, and any potential harm
4. *Notifications* – Who has been notified and notification evaluation e.g. have parents been notified, when – all parents or just those affected, evaluation of ICO notification decision
5. *Evaluation/Conclusion* – Report completed in conjunction with the Headteacher on effectiveness of response, investigation, mitigating factors, improvement to risk management, lessons learned

Guidance will be reviewed by LLD after each event and lessons learned communicated appropriately. Examples of events and weaknesses could include:

- Breach of physical security eg. intrusion into premises/filing cabinet, theft of portable device
- Breach of Information Security Policy eg. sharing passwords, displaying passwords on computer
- Security threat eg. hacking, loss of data
- Unauthorised access eg. identity theft, breach of data protection principles
- Internet related eg. inappropriate social networking, inappropriate sites
- E-mail related eg. inappropriate use of email
- Software malfunction
- System security weakness
- Multiple other eg. loss of USB key

Disposal of Redundant ICT Equipment Policy

All redundant ICT equipment will be disposed of correctly through the disposal scheme recommended by the Flintshire Education ICT Unit. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data if appropriate.

The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal. The school's disposal record will include:

- Date of disposal
- Authorisation for disposal, including whether any personal data is likely to be held on the storage media. If personal data is likely to be held the storage media will either need to be over written multiple times to ensure the data is irretrievably destroyed or physically damaged by the authorised disposal agent. Responsibility for appropriate destruction and compliance with Principle 7 of the Data Protection Act remains with the Data Controller of the school.
- How it was disposed of eg waste, gift, including details of data cleansing
- Name of person and/or organisation who received the disposed item
- Copy of receipt of acceptance of responsibility for destruction of personal data where appropriate

Any redundant ICT equipment being considered for gifting will have been subject to a recent electrical safety check and hold a valid PAT certificate.

All portable storage items such as memory sticks which fail should also be (safely) physically destroyed to prevent potential loss of sensitive data