Information Security Management Policy

Review Date	October 2015	**Leader of Policy Review**	Mr. S. Budgen

Information is precious. We are committed to preserving the confidentiality, integrity, and availability of our information assets:

- to deliver a quality education to the students within our care;
- to comply with the law;
- to meet the expectations of our parents, carers and the community;
- for sound decision-making;
- and to protect our reputation as a professional and trustworthy organisation.

Damage to any information we hold can cause problems for our school community. We have identified information management as one of our key risks and within this policy are implementing measures that help us to manage it. Information security is everyone's responsibility. We all need to make sure that we know how to use information safely and securely.

Information security means safeguarding information from unauthorised access or modification to ensure its:
Confidentiality – ensuring that the information is accessible only to those authorised to have access;
Integrity – safeguarding the accuracy and completeness of information by protecting against unauthorised modification;
Availability – ensuring that authorised users have access to information and associated assets when required.

Terms of the Policy

It is the Policy of the School to ensure that:

a) Confidential and personal information will be protected against unauthorised access.
b) Integrity of information will be maintained[1].
c) Regulatory and legislative requirements will be met[2]
d) Information governance maintained and tested
e) Information security education and training will be available to all staff.
f) Potential breaches of information security must be reported and investigated.

This means for the school that:

- All users of school information systems must be authorised to do so[3].
- 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 head teacher or designated person who is also responsible for providing advice and guidance on the implementation of this policy.
- The head teacher is directly responsible for implementing the policy within their school 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[4].
- Access / requests by 3rd parties must be carefully considered before allowing access to data.
- All breaches of this policy must be reported immediately to the Lifelong Learning Data Protection Officer.
- All serious breaches will be reported to the Information Commissioner's Office (ICO) with the assistance of the LLD Data Protection Officer.

NOTES
[1] Safeguarding the accuracy and completeness of information by protecting against unauthorised modification.
[2] This includes but is not limited to acting in accordance with the Data Protection Act 1998, Human Rights Act 1998, and Copyright, Designs and Patents Act 1988 and the recommendations of the Caldicott Committee.
[3] Ensuring that access to information and information systems is only granted to those who require it to perform their duties – see Appendix .
[4] Individuals in breach of this policy and supporting guidelines may be subject to disciplinary procedures

Information Security Management Policy

The School collects information about students and their parents or legal guardians. Information is also received from other schools when students transfer. The School uses the information it collects to administer the education it provides to students. For example;

- the provision of educational services to individuals
- monitoring and reporting on students' educational progress
- the provision of welfare, pastoral care and health services
- the giving of support and guidance to students, their parents and legal guardians
- the organisation of educational events and trips
- planning and management of the school

Information held by the School, LEA and the National Assembly for Wales on students, their parents or legal guardians may be shared with other organisations when the law allows, for example with;

- other education and training bodies, including schools, when students are applying for courses, training, school transfer or seeking guidance on opportunities
- bodies doing research for the National Assembly for Wales, LEA and schools, so long as steps are taken to keep the information secure central and local government for the planning and provision of educational services
- social services and other health and welfare organisations where there is a need to share information to
- protect and support individual students
- various regulatory bodies, such as ombudsmen and inspection authorities, where the law requires that information be passed on so that they can do their work

The sort of personal information that will be held includes;

- personal details such as name, address, date of birth, and contact details for parents and guardians
- information on attendance and performance in internal and national assessments and examinations
- information on the ethnic origin and national identity of students (this is used only to prepare summary statistical analyses)
- details about students' immigration status (this is used only to prepare summary statistical analyses)
- medical information needed to keep students safe while in the care of the school
- information about the involvement of social services with individual students where this is needed for the care of students

Transfer of such information to the LEA and WAG is via the Pupil Level Annual School Census (PLASC) that takes place three times each year. It is used for funding purposes, and to do research primarily to inform education policy changes. The research is done in a way that ensures individual students cannot be identified.

The LEA also uses the personal information collected to do research. It uses the results of the research to make decisions on policy and the funding of schools, to calculate the performance of schools and help them to set targets. The research is done in a way that ensures individual students cannot be identified.

The Data Protection Act 1998 gives individuals certain rights in respect of personal information held on them by any organization, and the School will try to ensure that information is accurate and secure.

Definition and Use of Personal data

The Data Protection Act applies to *personal data* (data that applies to a living person) held on a computer system or on paper. Stricter rules apply to *sensitive personal data* including (but not limited to) special educational needs, health (mental or physical), religious beliefs, racial or ethnic origin and criminal offences.

The first step for all organisations must therefore be to identify, within all the data they hold, which data counts as 'personal'. Personal data must be processed in accordance with certain principles and conditions.

Information Security Management Policy

Anyone who processes personal information must comply with eight principles, which make sure that personal information is:

1. fairly and lawfully processed
2. processed for limited purposes
3. adequate, relevant and not excessive
4. accurate and up to date
5. not kept for longer than is necessary
6. processed in line with the individual's rights
7. secure (appropriate technical security measures)
8. not transferred to other countries without adequate protection.

Personal data can only be processed under one or more of the following rules:

An individual has given consent
It is part of a contract
It is a legal obligation
It is necessary to protect the individual
It is necessary to carry out public functions
It is in the legitimate interests of the data controller.

While explicit consent must be obtained in many contexts, consent is not required for the purposes of delivering an education within the education sector. However, the reasons for collecting and processing sensitive personal data must be completely transparent.

It is a legal requirement to protect sensitive personal data. In an educational organisation, 'sensitive' personal data would include, for example, data recording that a pupil was considered 'at risk', or that a member of staff had had extended leave for mental health problems. Individuals entrusted with sensitive personal data, however derived, are accountable for its protection and compliance with the law.

Every item of personal data that is held or processed must be accurate, up to date and held for no longer than necessary. When personal data is no longer relevant to the purpose for which it was originally obtained, and/or has reached the end of the period for which it must legally be retained, it must be securely destroyed in accordance with its relevant protective marking.

Where the educational organisation has contracted a third party to manage all or part of information management through managed services, a policy will need to be in place covering the protection of personal or sensitive data.

Third Party Access to Data

Fax

- Consider whether sending the information other means other is secure e.g. encrypted or password protected e-mail
- Only send necessary information only
- Make sure you **double check the fax number** you are using. It is best to dial from a directory of previously verified numbers.
- Check you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office.
- If the fax is **sensitive**, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine.
- Ring up or email to make sure the whole document has been received safely.

- Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents

- The ICO has issued fines for incorrect/mistakes use of faxes

Telephone

- Check the individual is who you they claim to be
- Check they have parental rights or permission
- Only provide the minimum information
- Consider ringing them back

E-mails

- Consider whether the content of the email should be encrypted or password protected.
- When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - eg “Dave” - the auto-complete function may bring up several “Daves”. Make sure you choose the right address before you click send.
- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
- If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient’s

Police Access
Do police have an automatic right to personal information about pupils? No, but police have a right to request information required to investigate or prevent crime. An exemption form s29 must be completed by a police officer of the rank Inspector or above.

Relevant information sharing protocols or agreements should be in place e.g. WASPI 3. [Wales Accord on Sharing Personal Information]

Parents
Do parents have an automatic right to information – no some parents do not hold parental authority and information they may have access to may be limited. Young people may also be considered to understand a subject access request at the age of 12 and their wishes may have to be considered.

Grandparents
Do grandparents have a right to information – no they require parental permission.

All third party requests should be considered in accordance with schedule 2 and schedule 3 of the Data Protection Act.

Access, exit and staff awareness

Formal exit/handover procedures must be in place for all school staff who have access to school ICT systems and portable devices to ensure that they no longer have access to systems and applications e.g. SIMS and any personal data held by them is appropriately destroyed/returned. The Education ICT Unit helpdesk must be contacted to arrange for access to be removed. Staff in possession of a mobile device (laptop/memory stick/hard drive etc) must return any device as part of the formal exit procedure.

The formal procedures set out must be followed in order for school staff to have access to school ICT systems and portable devices.

Examples of Information Governance

It is advised that the head teacher or appropriate staff member attend the annual training opportunities e.g. heads conference, after school event dealing with Information Governance.

It is advised that Governors attend annual training opportunities dealing with Information Governance (in accordance with the Ministers suggestions that school governing bodies offer a more secure challenge to the schools and their staff).

It is advised that an annual review of AUP and Information Governance advice be undertaken with all staff at beginning of the academic year or with induction of new staff (minuted or evidence in some other way)