Ysgol Penyffordd

Polisi Diogelu Data
Information Security Management
(Data Protection) Policy

Cariad at ddysg.
A love of learning.

Ysgol Penyffordd Information Security Management Policy

Ysgol Penyffordd aims to safeguard the confidentiality and integrity of its information and to meet it's obligations under the Law. The outcome of the Policy is to protect the school's information from all threats, whether internal or external, deliberate or accidental.

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 E.
4. Individuals in breach of this policy and supporting guidelines may be subject to disciplinary procedures
5. See further guidance: Access to personal information by 3rd parties – Appendix B.

Contents:

Introduction.

The Data Protection Act 1998 came into force on 1 March 2000, bringing the UK in line with a European Directive on Personal Data (95/46/EC). The Act is there to protect the individual rights and freedoms of individuals, especially their right to privacy with respect to the processing of personal data.

The Data Protection Act 1998 requires all organisations, including educational organisations, to hold personal data securely. (see Appendix A)

Terms of the Policy

The School Management Team and Governing Body support the requirements of Information Governance and approve the Information Security 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[5].
- All breaches of this policy must be reported immediately to the 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 Policy

Objective: To achieve and maintain appropriate protection of school data.

Scope
This Policy applies to all portable devices. It applies to all staff users of the school's ICT systems.

Examples include (but not limited to):-
1. Laptops/Notebooks
2. Tablet devices/iPods/iPads/
3. Floppy disks
4. CD ROMs
5. DVDs
6. Memory Sticks
7. External Hard Drives
8. Memory Cards that are present in devices such as mobile phones, digital cameras, PDAs etc.
9. Other devices that have the capacity to hold electronic information e.g. MP3 Players, satellite navigation systems etc.

Responsibilities
Head teachers are 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.

Acceptable Use
Personal, confidential or school data must only 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.

Good practice:

1. Only copy data that you actually need i.e. copy individual files not complete folders; unnecessary rows/columns in spreadsheets must be removed; where possible anonymise data.
2. Ensure that your laptop or memory stick etc. is encrypted.
3. Security is your responsibility at all times. The device must not be left unattended at any time (e.g. in a coat pocket on a hook, in a car, plugged into a PC which is not attended by you, visible on a table or desk). You must endeavour to keep the device securely on your person (use a lanyard). If this is not possible then the device must be locked away securely when unattended.
4. Only transport what is necessary, even information you may not consider to be confidential can be dangerous in the wrong hands.
5. Report any lost or stolen devices to the Head teacher immediately.
6. Only store data for as long as necessary and delete from the device as soon as possible.

Further Advice & Support:

Information Governance – Advice and guidance on Information Governance issues can be obtained from the LLD Data Protection Officer.

Breaches of this Policy may result in disciplinary proceedings being brought.

Please Note:
For advice on disposal of redundant equipment, please see the ***Disposal of Redundant ICT Equipment Policy.***

Reporting Information Security Events Policy

Objective: To ensure information security events and weaknesses are communicated in accordance with the Lifelong Learning Directorate (LLD) Data Protection Breach management plan. To manage the event, learn from it and change processes wherever necessary.

Scope
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.

Procedure
All information security events and weaknesses must be reported immediately via either:

- Lifelong Learning Directorate (LLD) Data Protection Officer (01352702718)
- Lifelong Learning Directorate (LLD) Principal Learning Officer for ICT (01352704343)

Event will be managed using the:

5 point Data Protection Breach Management plan.

The (LLD) Data Protection Officer will visit the school who reported the event or weakness to gather the precise details. A central record of all information security events and weaknesses will be maintained by the (LLD) Data Protection Officer.

1 *Fundamental Details*
Contacts, & Incident Outline will be recorded immediately the incident is discovered. Appropriate Officers [see above] 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 system

3 *Data Risk Assessment*
What type of information, how sensitive. Who affected – number, consequences – how serious, how substantial, potential harm

4 *Notifications*
Who has been notified and notification evaluation
e.g. have parents been notified, when – all parents or just affected, Evaluation of ICO notification decision

5 *Evaluation/Conclusion*
Report completed in conjunction with the Head Teacher [Data Controller for the School] on effectiveness of response, investigation, mitigating factors, improvement to risk management, lessons learned.

Guidance will be reviewed by LLD and the schools after each event and lessons learned communicated appropriately.

Examples of events:
These are examples of events and weaknesses:
1. Breach of physical security e.g. intrusion into premises/filing cabinet, theft of portable device
2. Breach of Information Security Policy e.g. sharing passwords, displaying passwords on computer
3. Security threat e.g. hacking, loss of data
4. Unauthorised access e.g. identity theft, breach of data protection principles
5. Internet related e.g. inappropriate social networking, inappropriate sites
6. E-mail related e.g. inappropriate use of email
7. Software malfunction
8. System security weakness
9. Multiple
10.Other e.g. loss of USB key

Disposal of Redundant ICT Equipment Policy

Context:

Schools have a responsibility to have in place a scheme setting out how redundant ICT equipment will be disposed of within the rules of the Waste Electrical and Electronic Equipment (WEEE) directives.

Policy Aim:

All redundant ICT equipment will be disposed of correctly through an authorised agency or preferably, via 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.

Policy outline:

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.
- The school's disposal record will include:
    1. Date item disposed of
    2. Authorisation for disposal, **including whether any personal data is likely to be held on the storage media***
    3. How it was disposed of eg waste, gift, including details of data cleansing
    4. Name of person & / or organisation who received the disposed item
    5. Copy of receipt of acceptance of responsibility for destruction of personal data where appropriate

  * 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.

- 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

The Flintshire Education ICT Unit disposal scheme.

Procedure:

1. School informs ICT Unit on need for disposal of ICT equipment.
2. Education ICT Unit arranges collection of hard drive from all equipment.
3. After the hard drives have been removed and returned to ICT the equipment is then disposed of from the school through the recommended disposal company.
4. HDs are either re-formatted and re-used or are physically damaged (drilled) and disposed of through the recommended disposal company.

FAQs on Waste Electrical and Electronic Equipment (WEEE) are found in appendix D.

Appendix A - 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.

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. Responsibility for data security still rests on the educational organisation.

Appendix B - Remote Access to data including Schools/ICT Unit Remote Support Agreement

Use of remote access technology between the ICT Unit and Flintshire schools as stated on Technical and MIS Service Level Agreements:

- Schools allow ICT Unit staff to use remote access technology to:
  - provide support
  - upgrade/install software
  - investigate and solve problems
  - transfer files from school to school via the ICT Unit
  - configuration of data with prior agreement
  - extract data for investigation purposes by ICT Unit

- Remote access will only be used as necessary for undertaking the work outlined above and with the authority of the data controller

- All ICT Unit staff are subject to a regular enhanced CRB check

- ICT Unit staff will comply with the Data Protection Act in relation to sensitive data held on school computers.

- ICT Unit staff will keep a record of their use of remote access to include what was done and when and by who

Agreement

As part of the Policy, the following agreement must be completed and returned to the Education ICT Unit.

Name of School: Ysgol Penyffordd VA Primary School

I, Mrs J. Mulvey agree for the ICT Unit to use remote access procedures as outlined above and in accordance with the Service Level Agreements signed with the Authority.
Date:

I, Mr M. Rothero agree for the ICT Unit to use remote access procedures as outlined above and in accordance with the Service Level Agreements signed with the Authority.
Date:

Appendix C – 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 send dermatology report not asthma report available on the file.
- 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.

Appendix D - FAQ on Waste Electrical and Electronic Equipment directive

Q: What is WEEE and how does it affect me?

The WEEE directive came into force on 1st July 2007. It aims to minimise the impact of Waste Electrical and Electronic Equipment on the environment by increasing the re-use and recycling of old computers, electrical equipment, etc. thereby reducing the amount that goes into landfill sites.

For schools this means:

- No ICT equipment can be disposed of through the school's general waste collection process.
- Schools should have a policy setting out how redundant ICT equipment will be disposed of.

Q: I need to dispose of a computer that may have held personal or confidential data. Do I need to do anything to ensure I do not contravene the Data Protection Act?

Yes, Principle 7 of the Data Protection Act requires that technical and security measures must be taken to protect personal information. Breaches of the Data Protection Act may result in fines of up to £500,000.

Any computers, or storage media, that may have held personal or confidential data must either have their hard drives 'scrubbed' in a way that means the data can no longer be read or have these drives physically damaged - either before or as part of the disposal process.

It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data to ensure compliance with the Data Protection Act. The safest solution is to physically damage the hard drive beyond re-use.

Appendix E - 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 via the online control forms to arrange for access to be removed (see below). 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 by the Education ICT Unit must be followed in order for school staff to have access to school ICT systems and portable devices. The completion of the appropriate online form (see below) will be the only method used to notify the ICT Unit of changes to staff access. These should be used alongside this Policy so that all staff are aware of their responsibilities with regards to Information Governance.

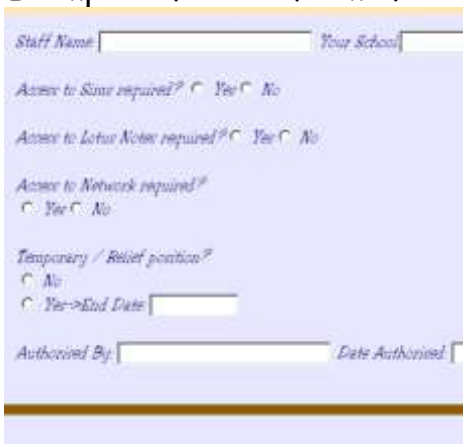
Examples of Information Governance.

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)

Examples of online forms for changing staff access to systems.



Do's and Don'ts

	Done?
• Do register as Data Controller & register all systems holding personal data with ICO	
• Do read the Information Management policy, sign up to it and then implement and monitor it.	
• Do assign authorised users a unique user ID and password - which then must not be shared under any circumstances.	
• Do identify a named individual for managing information security (usually performed by the head teacher or designated SLT member) who is also responsible for providing advice and guidance on the implementation of this policy.	
• Do make all staff aware of their responsibilities under the policy.	
• Do advise that it is a responsibility of each employee to adhere to this Information Security policy and all relevant supporting guidelines.	
• Do carefully consider access requests by 3rd parties before allowing access to data	
• Do consider what method you use to deliver personal data – e.g. only use fax as a last resort and use in accordance with guidance	
• Do report all breaches of this Policy immediately to the Lifelong Learning Data Protection Officer or the Principal Learning Officer for ICT.	
• Do sign up to the agreement allowing 3rd party access by support staff at the Education ICT unit to school's data and send back to ICT Unit.	
• Do encrypt ALL staff memory sticks and non-curriculum laptops and record that you have done so	
• Do dispose of redundant ICT equipment according to the guidelines offered i.e. use the ICT unit.	
• Don't ever store personal, sensitive data on an unencrypted mobile device	
• Don't transport data unnecessarily using mobile devices	
• Don't leave confidential material out for others to view, whether written, faxed or screen based.	
• Don't offer to share data on a pupil to a police officer	

unless they have submitted a S29 form signed by a senior officer of rank inspector or above	
• Don't email yourself personal, sensitive data from your school email account to another personal account	