E SAFETY

POLICY

Chair of Governors:

Date: 27/6/25

Review date: June 2028

E Safety Policy

Contents

Introduction

Ysgol Bryn Derw Special School believes that Information and Communication Technology is an integral part of learning to prepare our pupils for today's society. It is imperative that we equip them with evaluative skills to use the internet safely in and out of school. Recognising e-safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications.

> *"Children and young people need to be empowered to keep themselves safe – this isn't just about a top-down approach. Children will be children – pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim".*
>
> *(Dr Tanya Byron, 2008)*

Ysgol Bryn Derw Special School's E-Safety Policy has been written by the school, in accordance with Newport CC School Information Security Policy and government guidance. It has been agreed by the Senior Leadership Team and approved by the governors. It will be reviewed annually by the School Business Manager and the DSP.

Use of the internet

Internet use is a statutory part of the National Curriculum in Wales and a necessary tool for learning. It is a part of everyday life for education, business and social interaction. Our school has a responsibility to provide students with Internet access as part of their learning experience. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

Benefits

Some of the benefits of internet access in the school are, but not limited to as follows:

Access to national and worldwide educational resource.

- Access to experts in many fields via email and online conferencing and communications.
- Professional development for staff through access to national developments, 14-16 digital learning materials, the South East Wales consortium and other national sources of CPD support.
- Exchange of curriculum and administration data with Newport City Council and within Ysgol Bryn Derw Special School.
- Anytime and anywhere access to learning.

Enhancing learning

The school's Internet access will be designed to enhance and extend education. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Our school will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law.

Evaluating content

The evaluation of online materials is an essential part of the teaching and learning across all subject areas. Staff will evaluate web content and applications used in lessons and activities for suitability before giving access to pupils. Pupils will be clear on the school procedures for reporting unsuitable content. (see Acceptable Use Agreement).

MANAGING SYSTEMS

USE OF EMAIL

- Pupils at Ysgol Bryn Derw may only use the approved school email accounts provided by Hwb/Newport City Council Shared Resource Service (SRS) to communicate during school time for purposes related to education unless agreed by the Headteacher.
- Pupils should inform a member of staff as soon as possible if they have received an offensive email.
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission from school staff.
- Pupils are not allowed to access their own personal email or communication accounts using the school network system.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Staff should only use school email accounts to communicate with pupils as approved by the Senior Leadership Team.
- Staff should not use personal email accounts during school hours or for professional purposes.

MANAGING PUBLISHED CONTENT

Ysgol Bryn Derw's website has been created to celebrate pupil's work, promote the school and communicate events and projects with the wider community. The website will only be used to communicate public information of which should be considered from a school security viewpoint.

The contact details on the school website are the school address, email and telephone number. No other email addresses are to be published on the school website. Staff or pupils' personal information must not be published.
The website should comply with Ysgol Bryn Derw's guidelines for publications including respect for intellectual property rights and copyright.

In order to further secure pupil's personal information, the publishing of full pupils' names with their images is not acceptable on Ysgol Bryn Derw's website.
Pupils must have parental permission before their work or photograph can be published on Ysgol Bryn Derw's website.
Images that include pupils will be selected carefully and will not provide material that could be reused.

SEESAW

Ysgol Bryn Derw will use Seesaw to communicate information, pictures and videos to parents. Seesaw is a private communication channel between the school and individual parents/carers. All parents/carers will need to sign an agreement to give permission for Seesaw to be used, and for their child to be photographed/filmed individually, or both individually and in a group. If group consent is given, no names or personal information about other children will be shared.

Managing social networks

PUPILS

Most social networking sites/ email accounts and the like, state that a person has to be aged 13 or over to have an account. Under no circumstances should teachers or staff authorise such an account for pupils and should endeavour to educate pupils in this area to raise awareness.

Only social networking sites/ email accounts authorised by senior leadership team are to be used in school.

Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM (Instant Message) and email addresses, full names of friends/family, specific interests and clubs etc.

Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.

Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

ALL STAFF

Staff should be advised not to run social network spaces for pupil use on a personal basis.

If personal publishing is to be used with pupils, then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should be moderated by school staff.

Staff and pupils will be advised on security by the DSP and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Staff and pupils should be encouraged to invite known friends only and deny access to others by making profiles private.

Staff should be reminded of the Newport City Council e-Safety Policy and Guidance documents that refer to;

Code of Professional Conduct and Practice for Registered Teachers
Code of professional conduct and practice and The School Information Security Policy. (Appendix 2)

MANAGING FILTERING

Ysgol Bryn Derw will work with Newport City Council and the Shared Resource Service (SRS) to ensure that systems to protect pupils are reviewed and improved.

If staff or pupils discover unsuitable sites, the URL must be reported to the e–safety Coordinator.

The school's broadband access will include filtering appropriate to the age and maturity of pupils via the SRS Smoothwall system.

Senior staff along with the SRS and advisory support will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any material that the school believes is illegal must be reported to appropriate agencies such as Internet Watch Foundation (IWF) or the Child Exploitation and Online Protection centre (CEOP).

The school's access strategy will be designed by teachers and educators to suit the age and curriculum requirements of the pupils, with advice from SRS.

MANAGING EMERGING TECHNOLOGIES

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Staff will be issued with a school phone where contact with pupils is required.

Mobile phones will not be used during lessons or formal school time unless authorised by the Senior Leadership Team for a curriculum related activity.

Other devices, such as iPods and iPads that connect to the internet should be used with clear guidelines set by the class teacher and the internet accessed through the school network only.

The protection of personal data and GDPR (General Data Protection Regulation)

The GDPR 2018 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.

The school is GDPR compliant, and personal data will be recorded, processed, transferred and made available according to the GDPR 2018.

Policy decisions

AUTHORISING ACCESS TO THE INTERNET

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

(Foundation Phase)

Access to the Internet will be by adult demonstration and directly supervised access to specific, approved online materials.

Pupils should be able to access the internet independently under supervision by a member of staff.

Pupils and parents should discuss and agree and sign the Acceptable Use Agreement and have a clear understanding of e-safety rules for Ysgol Bryn Derw.
Parents will be asked to sign and return a consent form for pupil access. (Appendix 3)

Parents will be informed that pupils will be provided with supervised Internet access.

RISK ASSESSMENT

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Newport City Council can accept liability for the material accessed, or any consequences resulting from Internet use.

Ysgol Bryn Derw will audit ICT use to establish if the e–safety policy is adequate and that the implementation of the e–safety policy is appropriate.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

HANDLING E-SAFETY COMPLAINTS

Complaints of Internet misuse will be dealt with under our School's Complaints Procedure.

Any complaint about staff misuse must be referred to the Head Teacher. Any complaint about misuse by the Head Teacher must be referred to the Chair of Governors.

All e–safety complaints and incidents will be recorded by the school — including any actions taken. Pupils and parents will be informed of the complaints procedure.

Parents and pupils will work in partnership with staff to resolve issues.

Discussions will be held with the local Police Community Support Officer and/or Children's Safeguarding Team to establish procedures for handling potentially illegal issues.

Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

THE INTERNET IN THE COMMUNITY

The school will liaise with local organisations where necessary to establish a common approach to e–safety.

The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

All members of the community who use internet facilities within the school will complete an appropriate Acceptable Use Agreement. (Appendix 4)

MANAGING CYBERBULLYING

Cyber bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.

There are clear procedures in place to support anyone affected by Cyber bullying as set out in Ysgol Bryn Derw's Anti-Bullying Policy.

All incidents of cyber bullying reported to the school will be recorded.

There are clear procedures in place to investigate incidents or allegations of Cyber bullying:

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- Pupils, staff and parents/carers will be advised to not delete the offending texts, emails, video etc.

- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Sanctions for those involved in Cyber bullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at school for the user for a period of time.
- Parent/carers may be informed.
- The Police will be contacted if a criminal offence is suspected.

MANAGING LEARNING PLATFORM

The LA will monitor the usage of the Learning Platform (LP) by pupils and staff regularly in all areas, in particular message and communication tools and publishing facilities.

All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

Any concerns with content may be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the LA administrator if the user does not comply.
- Access to the LP for the user may be suspended.
- The user will need to discuss the issues with a member of Senior Leadership Team before reinstatement.
- A pupil's parent/carer may be informed.

NB *if a school uses another LP other than that provided by the LA then suitable provision has to be put in place for technical support and monitoring.)*

CLOUD STORAGE

Following National Guidance, Ysgol Bryn Derw will take steps to ensure that all personal details (names, addresses, photographs etc.) that are cloud stored will comply with requirements – for the data to be stored within the EU and comply with EU regulations. Contracts with companies for storage (e.g. Evolve) will be checked to ensure full compliance with these requirements.

Communication policy

PUPILS

All users will be informed that the network and internet will be monitored.

A programme of e-safety awareness activities will take place regularly in all year groups throughout the school year to raise the awareness and importance of safe and responsible internet access.

Useful websites for these purposes include:

Home - My Safety Net
Keeping children safe online | NSPCC
CEOP Education
Looking for Kidsmart? | Childnet
Pupil instruction in responsible and safe use will precede Internet access.

Safe and responsible use of the internet and technology will be reinforced across the curriculum, covering both home and school access. Particular attention will be given where pupils are considered to be vulnerable.

Acceptable Use Agreement will be attached to the e-safety rules when sent out with annual permission forms in September of each year. (Appendix 3)

STAFF

The E-Safety Policy will be formally introduced and discussed with staff and governors.
To protect all staff at Ysgol Bryn Derw, each member will be asked to sign an Acceptable Use Agreement (Appendix 1) which addresses in detail the 'dos' and 'don'ts' of staff usage of ICT and technology. Each laptop and desktop device is configured to remind the user of the agreement prior to its use and has to be accepted in order for the user to sign in to that device.
Staff are reminded that it is the duty of all staff in school to report any concerns they have about the use of misuse of technology or inappropriate use of ICT/Social Media
All staff are to be aware that internet traffic can be monitored and traced back to the individual user. Discretion and professional conduct is essential.

PARENTS

Parent and Carers attention will be brought to the e-safety policy in newsletters, Ysgol Bryn Derw 's brochure and on the school website.

Ysgol Bryn Derw will actively provide demonstrations and suggestions for safe home Internet use or highlighting e-safety at specific workshop session or other attended events e.g. parent evenings, sports days.

Parents will be requested to sign an e-safety/internet agreement as part of the Home School Agreement.

Information and guidance for parents on e-safety will be made available to parents in a variety of formats.

This policy will be reviewed annually by the School Business Manager and DSP.

POLICY REVIEW

This policy will be reviewed by Governors within 3 years of approval, or sooner if legislation/best practice requires

Appendix 1:

ICT Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT.

I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

I understand that Ysgol Bryn Derw will monitor my use of the ICT systems, email and other digital communications.

I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE, portable devices) out of school.

I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

I will only send emails to external organisations that are written carefully and authorised before sending, in the same way as a letter written on school headed paper.

I will only use school email accounts to communicate with pupils as approved by the Senior Leadership Team.

I will not use personal email accounts during school working hours or for professional purposes.

I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the Ysgol Bryn Derw policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so by Senior Management. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

I will only use chat and social networking sites in school in accordance with the school's policies.

I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner.

I will only use official blogs or wikis that are password protected and run from the school website with approval from the Senior Leadership Team. I am advised not to run social network spaces for pupil use on a personal basis.

I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) at Ysgol Bryn Derw, I will follow the rules set out in this agreement, in the same way as if I was using Ysgol Bryn Derw school equipment. I will also follow any additional rules set by Ysgol Bryn Derw about such use (see E-safety Policy). I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
I will not use personal email addresses on the school ICT systems.
I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
I will ensure that my data is regularly backed up, in accordance with relevant school policies.
I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
I will not disable or cause any damage to school equipment, or the equipment belonging to others.

I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school's Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
I understand that when I leave the school my accounts or rights to specific school areas will be disabled or transferred to my new establishment.
I understand that data protection policy requires that any staff or student data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Ysgol Bryn Derw school policy to disclose such information to an appropriate authority.
I will immediately report any damage or faults involving equipment or software, however this may have happened.
When using the internet in my professional capacity or for Ysgol Bryn Derw sanctioned personal use:
I will ensure that I have permission to use the original work of others in my own work
Where work is protected by copyright, I will not download or distribute copies (including music and videos).
I understand that I am responsible for my actions in and out of school:
I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment at Ysgol Bryn Derw, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use Ysgol Bryn Derw ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: ________________________________
Job Title: ______________________________
Signed: _______________________________
Date: __________________________________

Appendix 2:

School Information Security Policy

2021-22

NEWPORT CITY COUNCIL - EDUCATION SERVICE

School Information Security Policy

Table of contents

1. Security policy

Background and purpose

In order to ensure the efficient and effective delivery of school services we are making ever increasing use of information and communication technology (ICT) and of pupil, financial and other information held by us, the local authority (LA) education services and other public sector organisations.

We recognise that the information we hold, process, maintain and share with others is an important asset and that, like other important business assets, needs to be suitably protected.

In order to build public confidence and ensure that the school complies with relevant statutory legislation, it is vital that we maintain the highest standards of information security; this Information Security policy sets out the school's approach.

PSN is the **P**ublic **S**ervices **N**etwork (formerly GCSx) is a secure private wide-area network (WAN) which enables secure communications between connected local authorities and other public sector organisations. To connect to this secure network, Newport City Council must comply with the key controls which have been defined by central government. Schools are connected to the Newport City Council network and therefore need to take appropriate measures to protect the network overall.

The policy is divided into sections which provide a set of controls on which this policy is based. Where there are links to other policies, the security policy will highlight the key elements and link to the appropriate guidance or policy document which should be read in full.

2. Security Organisation

2.1 Information security is a responsibility of everyone and is shared by the senior leadership team.

2.2 The Local Authority Information Management team is the appointed Data Protection Officer (DPO) for Newport Primary Schools. Newport High Schools will need to appoint a DPO for their schools.

2.3 The school governors will appoint a Senior Information Risk Owner (SIRO) to oversee all aspects of information security. The SIRO will, in turn, appoint Information Asset Owners (IAO's) who will be responsible for individual information assets, such as the attendance data, exam data etc. Typically, the SIRO will be a member of the senior leadership team.

2.4 The DPO, SIRO and IAO's will conduct periodic risk assessments of identified risks, compiling these into a Risk Register. The National Archives has published guidance around these roles.

2.5 The DPO, SIRO and IAO's will be responsible for adopting and developing information security policies and guidance, together with training and communicating those policies to reduce information risks. The intention is to provide standard policies that schools can adopt or amend. This will be based on existing corporate policies although they will require review and amendment.

2.6 Physical access to the school's IT facilities by third party suppliers might present a security risk. Where there is a business need for such access, the third party should be escorted at all times.

2.7 Remote access to school data by non-employees (including parents) will be carefully considered after consultation with the council's education service and the school's IT department where necessary to ensure appropriate safeguards are in place that would not compromise the overall integrity of the school system. If this action is allowed then clear guidelines will be devised and shared with these groups to ensure safe and responsible use is maintained, with explicit sanctions published where safety is compromised.

3. Information Security

3.1 Security must be addressed at the recruitment stage and included in job descriptions, contracts, and all induction courses. Job descriptions should define security roles and responsibilities as laid down in the *school's information security policy*. This should include any general responsibilities for implementing or maintaining the School's security policy, as well as any specific responsibilities for the protection of systems or for the execution of security processes. This is an area of perceived weakness to be addressed generally.

3.2 Information security must be included as part of all induction courses and the school's policies on IT security must be covered. To ensure the integrity of all the school's data, staff should have received training on any application that they would be required to access and any software package they will be required to use in line with the Acceptable Use Policy.

3.3 **All information security incidents and data breaches must be reported immediately**. **The Information Commissioners Office (ICO) will need to be informed of serious breaches within 72 hours.** It is important that all employees, contractors and parents / volunteers are aware of the procedure for reporting the different types of incident – security breach, threat, weakness, or malfunction – that might have an impact on the security of the schools' data or assets. Primary Schools must follow the corporate information security incident reporting procedure. High Schools should consider adopting an amended version of the corporate incident reporting policy. Schools must also report any observed or suspected incidents as quickly as possible to the school's SIRO. An investigation under the school's disciplinary code may be required.

3.4 Whilst every effort will be taken to ensure information security breaches or incidents do not occur, it is recognised that a clear incident reporting policy is necessary for the school.

Security incidents can be summarised as, but not limited to:

- **Loss or disclosure of personal data** such as leaving a document in an inappropriate area or emailing the wrong person.
- **Technical incident** such as loss of IT equipment or unauthorised access to the school network
- **Criminal incident** such as theft or attempted theft

3.5 Should an incident occur, the user will immediately report the facts to the DPO, Information Management team and/or SIRO as appropriate, who will arrange for the issue to be promptly investigated. A log of such incidents will be maintained and reviewed periodically to ensure that lessons are learned. The SIRO may have to report the incident to the Information Commissioner's Office (ICO). For further guidance, please contact the Information management team.

Information.management@newport.gov.uk

3.6 Everyone must be aware that the effects of loss or disclosure of sensitive information can lead to:

- A failure for the school to meet legal obligations
- A failure to meet public expectations
- Negative publicity / embarrassment
- Financial loss
- Disciplinary action or appropriate sanctions
- Fines being imposed by the ICO

3.7 By being security conscious, all employees and other individuals can contribute to the security of the information held by the school, which is an important part of information risk management.

Should an incident occur, by promptly following procedures listed in the policy, employees can minimise the potential impact of the security incident both on the school and on themselves.

3.8 Formal disciplinary procedures may be invoked against staff who have allegedly violated the school's security policy and procedures. The process will be a deterrent to employees who might be inclined to disregard security procedures and ensures a correct and fair treatment for those who are suspected of committing serious or persistent breaches of security. The school's standard disciplinary processes and procedures refer.

4. Physical and Environmental Security

It is recognised that a secure school and premises is also needed to support the overall security of school information.

4.0 Visitors must always be signed in and escorted as necessary.

4.1 Staff will be issued with identity badges which will be always worn whilst on school premises.

4.2 All servers and comms machines will be locked away and be accessible only to authorised IT staff.

4.3 Ensure that any areas and/or offices containing sensitive information are locked when not occupied.

4.4 All portable devices (e.g. laptops) will be held securely with signing in/out records to track usage and whereabouts.

4.5 The school will ensure that all hard copies of sensitive data are stored in appropriate filing systems and locked as appropriate. The school will ensure that only authorised staff have access to these filing systems.

4.6 The school will ensure that sensitive documents are not left where visitors or pupils could view them, for example receptionist's desks or pinned to notice boards. When printing out information, sensitive documents must be collected immediately and consideration should be given to using a secure printing service, or a local printer.

4.7 Consideration should be given to what documents it is appropriate to take out of the school and appropriate measures taken to ensure they are kept secure. Paper documents will need to be taken from school premises from time to time, but this should be kept to a minimum. Paper files should not be stored in laptop cases. The use of electronic files on encrypted devices is encouraged wherever possible.

4.8 Sensitive documents should be destroyed in line with the Newport City Council Information Retention and Disposal Policy which could be revised as appropriate and adopted by individual governing Bodies. Specific guidance for schools is provided by the Information and Records Management Society

4.9 The authority has a responsibility under the Government legislation (WEEE directive) and internal financial and security policies to dispose of all electronic equipment in a secure and environmental manner. All electronic equipment will be destroyed in line with the disposal of it equipment / mobile phones policy which could be revised and adopted by schools.

Schools with a managed service provided by the SRS can contact the SRS Team for disposal; non managed schools should contact the equipment suppliers for details. For further guidance contact the SRS service desk on 210210.

5. Computer and Network Management

5.0 All systems are subject to documentation requirements, these will be held securely.

5.1 Incident and problem management processes are operated to ensure effective response to security incidents and ICT issues.

5.2 Formal change control processes are in place to satisfactorily control all changes to equipment, software, and procedures. Such processes are designed to minimise the risk of problems occurring by suitable planning and implementation. All change requests should be submitted to the SRS for formal consideration and planning. Non-SRS supported schools should contact their IT providers.

5.3 Virus detection and preventions measures, and appropriate user awareness procedures are in place. This is provided to Schools with a managed service provided by the SRS and is required as part of non-managed contracts with external suppliers.

5.4 Adequate data backups must be taken to ensure essential data can be recovered in the event of a computer disaster or media failure. Schools with a managed service provided by the SRS have backups every night, which are cycled so a copy is always held off site.

5.5 In order to maintain acceptable levels of wide and local area network integrity and performance, it will be necessary for all system elements to be of a standard approved by the SRS in line with any local authority standards.

- Network equipment will be installed and maintained in accordance with current and appropriate British and International Standards and codes of practice.
- Be of a standard approved by the SRS.
- Not be adapted or altered in any way without prior consultation or agreement with the SRS.
- Utilise hardware components that have been approved by the SRS.

5.6 Council issued mobile phones are subject to the Mobile Communications Policy which can be revised as appropriate and adopted by individual Governing Bodies. Mobile devices should always be kept secure. Devices with cameras should only be used for taking work related pictures in line with the school's guidance on the use of photography. Mobile phone usage outside of the UK must be authorised in advance due to the cost and potential security issues.

5.7 Information Asset Owner's (IAO's) will maintain responsibility for the information and related system(s) that contain or process it.

5.8 Security measures for school information must take account of school needs for sharing and restricting information and the impacts on the school should unauthorised access be gained. Consideration must be given to the following school needs:

- **Confidentiality** - the need to share or restrict access to information with regard to confidentiality, and the necessary controls required restricting such access.
- **Integrity** - the controls and processes required maintaining and protecting the accuracy and completeness of data.
- **Availability** - information should be available when required but must be subject to any security procedures in place to protect the data.

5.9 Output from IT systems that contain confidential information (such as printouts) must be held in a secure area until collected by the owner.

Please also refer to **Appendix C – Sensitivity of Data**

6. System access control

6.1 Access to school IT systems is controlled through a formal registration process, which may involve completion of a form. Usage of these systems is recorded against the unique user ID. The IT provider must be informed of any staff joining, leaving, or changing roles to insure that user accounts are up to date and appropriate.

6.2 Staff termination processes will ensure that all identification badges, keys and school equipment etc. are returned promptly for all leavers in accordance with the council termination process.

6.3 All computer access will be promptly terminated on the user's last working day. Shared passcodes (e.g. to secure door areas) are required to be changed after any member of staff leaves.

6.4 To ensure only appropriate users have access to school data the following safeguards will be in place:

- Users with access to sensitive information must use **strong** passwords. • Passwords must be protected at all times and will be routinely changed.
- User access rights must be reviewed at regular intervals.
- It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to school systems.
- Partner agencies or 3rd party suppliers must not be given details of how to access the school's / council's network without approval from the SRS/IT Provider.

6.5 To assist, governing bodies could consider adopting the council's Password Policy.

7. Compliance and audit

7.1 The school has a responsibility under vendor licencing contracts to ensure all products are used within the respective terms and conditions. Where software is provided by the Local Authority then appropriate licence agreements will have already been sought.

7.2 Under no circumstances should personal or unsolicited software be loaded onto a school computer.

7.3 All software is required to have a licence and the school will not condone the use of any software that does not have a licence.

7.4 Unauthorised changes to software must not be made, and users must not attempt to disable or reconfigure the personal firewall or other security software.

7.5 Unauthorised use and illegal reproduction of software is subject to civil damages and criminal penalties.

7.6 The school will ensure compliance with the Data Protection Act 2018, Freedom of Information Act 2000 and any other related information security statutory responsibilities. Schools may use or amend the corporate Data Protection Policy if required.

7.7 The school will register with the Information Commissioner's Office (ICO) and will issue a privacy notice. The Information Management team will manage Primary schools ICO subscription upon agreement with each school and assist all primary schools with the publication of privacy notices.

7.8 Data should not be held for any longer than required and should be securely disposed of in accordance with the retention policy. For further details see 4.8 above.

8. IT Infrastructure

8.1 The SRS or school's IT provider will undertake technical separation of office and classroom machines from the council network and will undertake any necessary enhanced security on office machines.

8.2 The school's IT infrastructure will be maintained by the SRS or school's IT provider where all technical requirements can be discussed with the service providers and advice given as necessary.

9. Acceptable use policy

9.1 All IT users will sign an acceptable use policy, as this gives clarity to all parties regarding roles and responsibility of IT access and information / data usage.

9.2 All staff and users will be periodically issued with a 'dos and don'ts sheet' (**Appendix B**) to enhance user education and awareness and to assist in reducing the possibility of a data breach within the school.

9.3 An example School's Acceptable Use Policy is reproduced at **Appendix A**. Consideration should be given to reviewing and adopting the council's policy.

10. Email - acceptable use

10.1 All emails that are used to conduct or support official school business must be sent using the school's official email system or the secure Hwb portal provided by Welsh Government.

10.2 Non-work email accounts must not be used to conduct or support official school business.

10.3 Email correspondence which contains sensitive information will be encrypted before transmission to avoid a data breach should the email be mis-delivered. For further support or guidance about encryption, please contact the Information Management team.

10.4 Automatic forwarding of email must be considered carefully to prevent sensitive material being forwarded inappropriately.

10.5 Consideration should be given to reviewing and adopting the council's policy.

11. Internet acceptable use

11.1 At the discretion of the head teacher, and provided it does not interfere with your work, the school permits personal use of the Internet in your own time (for example during your lunchbreak). Governing bodies should consider the council's internet acceptable use policy which can be reviewed and adopted by individual schools.

11.2 Users are responsible for ensuring the security of their account log-on id and password. Individual user log-on id and passwords should only be used by that individual user, and they should be the only person who accesses the Internet via their account.

11.3 Users must not create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.

11.4 Users must assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.

11.5 Employees should comply with the requirements of the social media policy.

11.6 No filtering system can guarantee 100% protection against access to unsuitable sites. The school will monitor the activities of users on the system to identify issues.

12. Sensitivity of data

12.1 The information that the schools handle varies in levels of sensitivity. **Appendix C** sets out the sensitivity levels that the school has in place, based upon the government protective marking scheme.

12.2 **Official - sensitive** information is deemed to be highly sensitive and mission critical information for limited consumption. In these cases, the information will not be available beyond school electronically.

12.3 **Official** information is deemed to be essential to the successful running of the school, much of which can be accessed via the private side of the school's own learning platform. In these cases, access to this information will be via personal logon which will be granted to only those users who need access to perform their duties.

12.4 **Unclassified** information is deemed to be generally within the public domain and accessed via the public facing website or learning platform. Minimum security will be afforded to this information as there is no risk of data breach.

12.5 Information deemed to be **official** and **official - sensitive** must not be held on personal laptops, computers, tablet devices or pen drives as the disposal and maintenance routes for these pieces of equipment cannot be controlled and may therefore leave sensitive school data at the risk of unauthorised disclosure / exposure.

12.6 The primary storage of all school data and information will be on the school network which is backed up daily and can be accessed remotely if necessary.

13. Movement of Data

13.1 It is recognised that the use of data pens, laptops and tablet computers leads to a higher risk of data breaches through the loss / theft of this equipment.

13.2 Sensitive pupil information such as PLASC returns, new starters and leavers should only be transmitted or received via approved secure mechanisms including the DEWi or S2S systems.

13.3 If data must be moved from the school network, then the movement must comply with the school's information sensitivity table (**Appendix C**). In the case of information classed as official – sensitive or official, this will only be by using secure encrypted data pens or OneDrive secure email; this will greatly reduce the risk of data loss / data breach should a device be mislaid, lost or stolen. Instructions on the use of Microsoft One Drive and Message Encryption can be viewed here.

14. Remote access to school's network

14.1 Remote access to the school's own network is available to all staff and learners for those schools with a managed service provided by the SRS and should be considered standard for those needing to access school information and data beyond the school. This access negates the risk caused by removing data from the school.

14.2 Remote access to school data by non-employees (including parents) will be carefully considered after consultation with the council's education service and the SRS / school's IT service where necessary to ensure appropriate safeguards are in place that would not compromise the overall integrity of the school system. If this action is allowed then clear guidelines will be devised and shared with these groups to ensure safe and responsible use is maintained, with explicit sanctions published where safety is compromised.

15. Cloud services

15.1 Where sensitive or personal information is stored, the school will ensure that the cloud service provider complies with the Data Protection Act 2018 and the National Cyber Security Centre (NCSC) cloud security principles. A Data Protection Impact Assessment may be required, and Primary schools may consult with the Information Management team as appropriate.

16. Bring Your Own Device (BYOD)

16.1 The school will ensure that devices permitted to connect to the BYOD or Guest access networks have suitable antivirus and / or firewall software. Guidance should be sought from the SRS / IT service where necessary.

16.2 The school will ensure that sensitive data is not stored on personal or privately owned devices (see section 15)

16.3 BYOD equipment will be subject to the schools internet filtering and monitoring software or appliances.

16.4 Devices are brought into school at the risk of the owner.

16.5 The school does not accept responsibility for any malfunction of a device due to it connecting to BYOD or Guest access.

17. Biometric systems

17.1 The school will ensure that all biometric systems comply with UK GDPR and The Protection of Freedoms Act (2012). Guidance around the use of Biometrics has been developed by the Education service in conjunction with Information Management. For information, a draft guidance note has been produced.

18. Linkages with other guidance

18.1 Any local authority produced literature on this / related subject will be considered in full and, if appropriate review current procedures in line with recommendations.

19. Help and support

19.1 The local authority will be available to offer help and support for any information security queries via information.management@newport.gov.uk

20. Policy compliance

20.1 If any user is found to have breached this policy, they may be subject to investigation under the school's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

APPENDIX A – ACCEPTABLE USE POLICY

COMPUTING FACILITIES

Users are encouraged to make use of the school's computing facilities for educational purposes. All users are expected to act responsibly, show consideration to others, and not tamper with the equipment provided in any way.

Schools with a managed service provided by the SRS can access internal systems remotely. Guidance and support has been issued separately and schools should refer to this.

ACCOUNT SECURITY

Users are responsible for the protection of their own network account and should not share their passwords with anyone.

Passwords should be complex. It is recommended a minimum of 8 characters are used and should include uppercase and lowercase letters, numbers, and punctuation marks.

Users should not logon to or use any account other than their own and should logoff when leaving a workstation. In some situations, generic classroom accounts may be appropriate.

USE OF FACILITIES

It is not acceptable to:

- Attempt to download, store, or install software on school computers unless authorised by the SRS/Schools IT service.
- Attempt to introduce a virus or malicious code to the network.
- Attempt to bypass network or system security.
- Access or attempt to access another user's account.
- Attempt to gain access to an unauthorised area or system.
- Attempt to use any form of hacking/cracking software or system.
- Attempt to use proxy bypass or avoidance software or websites
- Use any device that acts as a Wireless Access Point (WAP), bridge or router
- Use any device that has access to the Internet via a connection that has not been provided via Newport City Council procurement channels.
- Access, download, create, store or transmit material that; is indecent or obscene, could cause annoyance or offence or anxiety to others, infringes copyright or is unlawful or brings the name of the school or Newport City Council into disrepute.
- Engage in activities that waste technical support time and resources.

INTERNET ACCESS

The school's internet service is filtered to prevent access to inappropriate content and to maintain the integrity of the computer systems. Users should be aware that the school logs all Internet use and reports of this can be made available.

- The use of public or private chat facilities is not permitted. The use of corporate chat facilities such as Microsoft Teams is permitted for appropriate schoolwork activities and communications.
- Users should not copy and use material from the Internet to gain unfair advantage in their studies, for example in coursework.
- Users should ensure that they are not breaking copyright restrictions when copying and/or using material from the Internet.

EMAIL

Automated software scans all email and blocks those that could compromise the integrity of the computer systems or contain unsuitable/offensive content. Users should be aware that the system logs all e-mail content.

- Pupils are not allowed to use email during lessons, unless the teacher for that lesson has permitted its use.
- If a user receives an email from an unknown person or that is offensive or upsetting, the relevant teacher or a member of the SRS / IT department should be contacted. Do not delete the email in question until the matter has been investigated.
- Sending or forwarding chain emails is not acceptable.
- Sending or forwarding emails to many recipients is acceptable only in certain agreed circumstances. Before doing so, the user must obtain permission from the SRS, School's IT department or School's Network Manager.
- **Do not open attachments or links from senders you do not recognise, or that look suspicious.**
- Users should periodically delete unwanted sent and received emails.
- Pupils may only use the email facilities provided by the School.

PRIVACY AND PERSONAL PROTECTION

- Users must always respect the privacy of others.
- Users should not forward private data without permission from the author.
- Users should not supply personal information about themselves or others via the web or email.
- Users must not attempt to arrange meetings with anyone met via the web or email.
- Users should realise that the school has a right to access personal areas on the network. Privacy will be respected unless there is reason to believe that the IS Acceptable Use Policy or school guidelines are not being followed.

DISCIPLINARY PROCEDURES

Those who misuse the computer facilities and break this acceptable use policy will be subject to school disciplinary procedures.

SUPPORT

If you have any questions, comments, or requests with regards to the systems in place, please do not hesitate to contact a member of the school's IT provider / SRS.

Faulty equipment should be reported to the SRS / school's IT provider. Users should not attempt to repair equipment themselves.

APPENDIX B – Do's and don'ts sheet

"Information security is about maintaining:

- **Confidentiality** – ensuring only people who have right to see the information can actually do so;
- **Integrity** – making sure that the information is right; and
- **Availability** – making sure that the information is always there when needed, and to the appropriate person." WAG, 2008.

Do	Don't
• I agree to the most recently published school's Acceptable Use Policy and I accept that my use of the computer network and associated applications may be monitored and / or recorded for lawful purposes.	• I will not use a colleagues login details or share mine with anyone.
• I will lock my PC / laptop if temporarily leaving it unattended.	• I will not leave a PC / laptop logged in and unattended.
• I will protect any sensitive material to the same level as paper copies including using a secure print option when materials are being printed to a shared printer.	• I will not allow pupils to use a PC/laptop that is logged in with my username; I will always ensure that the student connects using appropriate credentials.
• Anything which needs to be shared will be shared through the teachers shared area(s), which may be password protected.	• I will not transfer any data which I know, or suspect, to have a high level of sensitivity, unless I need to and then only via an encrypted method.
• I will always check that recipients of email messages are correct before I send it.	• I will not remove equipment from the school premises without appropriate approval.
• I will protect others from seeing sensitive information or me entering my password.	• I will not leave my password in a place which is easily accessed by others.
• I will report any security incidents in line with the school's policy and procedures.	• I will not knowingly introduce a virus or other malware into the system.
• I will observe the school's Health and Safety policies and procedures.	• I will not disable anti-virus or malware protection provided on my machine.
• I will comply with the Data Protection Act 2018 and other statutory obligations.	• **I will not open any attachments of click links from senders that I do not recognise.**
• I will ensure that any sensitive information is securely disposed of (whether paper or IT based).	
• I will immediately notify the loss or theft of any equipment or information in line with the School's Incident Reporting Policy.	
• I will sign out any portable device so there is a clear and up to date record maintained.	

APPENDIX C – Sensitivity of data

> "You should secure any personal data you hold about individuals and any data that is deemed sensitive or valuable to your organisation. Your organisation should have someone who is responsible for working out exactly what information needs to be secured." Becta, 2009

Level of sensitivity	Examples of data	Possible level of protection
Official - Sensitive Highly sensitive and mission critical information for limited consumption.	• Child protection matters • Staff personal information • Statutory returns e.g PLASC • UPN	• Not available beyond school electronically. Encrypted with limited access to staff when approved by Head Teacher • Use approved secure tool including DEWi / S2S to transfer data • Locked away in appropriate filing system
Official Essential to the successful running of the school.	• Attendance information & EWO reports • Performance management information • Staff profiles and performance reviews • IEP's, IBP's, AEN support, statements, annual reviews • Financial Information	**Teacher access** • Login password • Limited to teacher accounts • Password protect files **SSO Administrative Access** • Login password • Limited to Administrative accounts • Secure areas **Parent / Career access** • Login to own child records only (if applicable) • School's MIS **Pupil access** • Login only to their own progress records
	• Pupil Behaviour logs and discipline records • Pupil personal information • Examination data • Pupil reports • Letters to parents • Minutes of meetings • Pupil performance • Reward's reports • 3rd party applications – ie Parent Pay	

Unclassified Much is in the public domain and accessed via the public facing website or learning platform.	• Lesson plans • Schemes of work • Teaching notes • School calendar, staff bulletins • School policies and procedures • Pupil work • Pupils learning logs • General school / class letters • Pupil Photographs (with parental consent)	• Pupil login • Password on specific files

Official is broken down into two subsections; the top level has a higher sensitivity and should be treated accordingly.

Created by: Stuart Fowler
Date: 01/06/2015
Reviewed by: Tariq Slaoui
Date: 29/10/2021

Document control

Version	Date	Author	Notes / changes
V1.1	21/08/2015 - 5/11/2015	Stuart Fowler	Amendments from original policy reviewed by team
V1.2	14/12/2015	Stuart Fowler	Review following stakeholder comments
V1.3	19/02/2016	Mark Bleazard	Final Review
V1.4	2/8/2016	Stuart Fowler	Follow up review
V1.5	29/10/2021	Tariq Slaoui	Review

Appendix 3:

ICT ACCEPTABLE USE AGREEMENT FOR PARENTS/CARERS

To support a safe and responsible digital learning environment, we ask all parents and carers to r the terms below. This agreement outlines your role in supporting your child's safe use of technology at school and at home for educational purposes.

By signing this form, you are confirming that you understand and support the school's expectations around the appropriate use of ICT (Information and Communication Technology), internet access, and digital devices.

Pupil Use of ICT

As a parent/carer, I agree to:

- Support the school in promoting safe, responsible, and positive use of technology
- Encourage my child to use digital devices and the internet for learning and not for inappropriate or harmful activities
- Ensure that my child respects the privacy, safety, and dignity of others when using technology
- Help my child understand the importance of keeping personal information private online
- Discuss with my child the importance of reporting inappropriate content or behaviour to a trusted adult or teacher

School Responsibility

The school:

- Provides filtered internet access and monitors use of its ICT systems
- Teaches online safety and digital citizenship as part of the curriculum
- Responds to breaches of acceptable use with appropriate action
- Respects pupils' privacy while balancing the need to safeguard all users

Parent/Carer Responsibility

I understand that:

- The school provides rules and guidelines for ICT use and will support my child to follow these
- Deliberate inappropriate or unsafe use of ICT by my child may result in restricted access, disciplinary action, or further contact with parents
- I am responsible for supervising my child's use of technology at home and ensuring that school devices are used appropriately (if applicable)
- If the school lends a device (e.g., for remote learning), I will ensure it is used safely, stored securely, and returned in good condition

Agreement and Signature

I have read and understood the Acceptable Use Agreement and support the school in promoting safe and responsible use of ICT and the internet.

Pupil Name:	Class:
Parent/Carer Name:	Date:
Signature:	

Appendix 4:

ICT ACCEPTABLE USE AGREEMENT FOR VISITORS

I understand that I must use school ICT systems in a responsible way, to ensure that there is n or to the safety and security of the ICT systems and other users.

For my professional and personal safety:

- I understand that Ysgol Bryn Derw will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE, portable devices).
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the Ysgol Bryn Derw policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so by Senior Management. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) at Ysgol Bryn Derw, I will follow the rules set out in this agreement, in the same way as if I was using Ysgol Bryn Derw school equipment. I will also follow any additional rules set by Ysgol Bryn Derw about such use (see E-safety Policy). I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school's Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.

- I understand that when I leave the school my accounts or rights to specific school areas will be disabled.
- I understand that data protection policy requires that any staff or student data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Ysgol Bryn Derw school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for Ysgol Bryn Derw sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a removal of access and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use Ysgol Bryn Derw ICT systems and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: ________________________________

Job Title: ______________________________

Signed: _______________________________

Date: _________________________________