Ysgol Uwchradd Casnewydd
Newport High School

E-Safety Policy

Polisi E-Diogelwch

This policy was adopted by the Governing Body in September 2017 and is due for review September 2020

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

Roles and responsibilities

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The designated Governor with responsibility for safeguarding will act as the E-Safety Governor.

Headteacher

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Digital Competence Coordinator and Network Manager.
- The Headteacher is responsible for ensuring that the Digital Competence Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Digital Competence Coordinator.

Digital Competence Coordinator

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy and reporting any concerns to their line manager
- Provides training and advice for staff
- Liaises with school technical staff
- Meets with the E-Safety Governor as required to discuss current issues and practices
- Monitors improvement actions identified through use of the 360 degree safe self-review tool

Network Manager

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets recognised e-safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network, internet, Virtual Learning Environment, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher for investigation and follow up if necessary

- that monitoring software / systems are implemented and updated as required

Teaching and Support Staff

All teachers and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the school e-safety policy and practices
- they have read, understood and signed up to the Acceptable Use Agreement
- they report any suspected misuse or problem to the Headteacher for investigation and any necessary follow up
- all digital communications with students, parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the e-safety and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students are guided to sites checked as suitable for their use
- student level data is not sent over the internet or taken off the school site unless safely encrypted or otherwise secured

Staff must also ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete

Designated Person for Safeguarding

The Designated Person for Safeguarding will deal with any child protection or safeguarding issues that arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming

- cyber-bullying

Students

- are responsible for using the school digital technology systems in accordance with the Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand how use of mobile devices and digital cameras safely. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about e-safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / VLE and on-line student records
- their children's personal devices in the school

Community users

Community users who access school digital systems or the VLE as part of the wider school provision will be expected to sign the Acceptable Use Policy before being provided with access to school systems.

Curriculum use

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum.

- E-safety is included in Computing and ICT, PSE and Welsh Baccalaureate lessons and is regularly revisited
- E-safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students are encouraged to adopt safe and responsible use both within and outside school
- Staff act as good role models in their use of digital technologies the internet and mobile devices

- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

E-Safety training

It is essential that all staff receive e-safety training to ensure they understand their responsibilities. Training will be offered as follows:

- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreement.
- The Digital Competence Coordinator and Designated Person for Safeguarding receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy will be presented to staff in the staff handbook.
- The Digital Competence Coordinator will provide advice, guidance and training to individuals as required.

Governors are able to take part in e-safety training and awareness sessions offered in school.

Technical – infrastructure, equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented:

- The school's technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher and kept in a secure place.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. The school has provided differentiated user-level filtering
- School network staff regularly monitor and record the activity of users on the school systems and users are made aware of this in the Acceptable Use Agreement.
- Users are required to report any actual / potential technical incident or security breach to the Network Manager.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- A policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

Use of digital and video images

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital or video images.
- Staff and volunteers are allowed to take digital and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital or video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published.
- Students' work can only be published with the permission of the student, their parents or carers.

Communication Technologies

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carer must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or social media must not be used for these communications.

- No reference should be made in social media to students, parents / carers or school staff
- Staff should not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

This policy should be read in conjunction with the:

- Safeguarding Policy
- Behaviour for Learning Policy
- Privacy Notice