**

**Canolfan Addysg Conwy**

**E-Safety Policy**

**Introduction**

The internet and other digital technologies permeate all aspects of life in our modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

At Canolfan Addysg Conwy, we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

**Roles and Responsibilities**

The following section outlines the e-Safety roles and responsibilities of individuals and groups within the school:

Headteacher and Senior Leaders Team:

* 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 is delegated to department leads.
* The Headteacher and the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.
* Ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.

Conwy ICT Services 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 (as a minimum) the required e-Safety technical requirements as identified by the Local Authority.
* that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
* 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, email is regularly monitored in order that any misuse can be reported to the Headteacher for investigation.

**Teaching and Support Staff**

Are responsible for ensuring that:

* they have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices
* they have read, understood and signed the Staff Acceptable Use Agreement
* they report any suspected misuse or problem to the Headteacher or SLT
* all digital communications with parents should be on a professional level and only carried out using official school systems
* e-Safety issues are embedded in all appropriate aspects of the curriculum and other activities
* pupils understand and follow the e-Safety and acceptable use agreements
* they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and implement current policies with regard to these devices
* in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

**Pupils**

* are responsible for using the school digital technology systems in accordance with the Acceptable Use Agreement
* need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
* 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, if related to their membership of the school

**Parents / Carers**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. 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:

* internet and mobile devices when out of school

**Policy Statements**

Education - Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach depending on their ability. The education of pupils in e-Safety is therefore an essential part of the school’s e-Safety provision and is adapted for pupils depending on their age and ability.

e-Safety should be a focus in all areas of the curriculum and staff should reinforce e-Safety messages across the curriculum. The e-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

* Key e-Safety messages should be reinforced as part of a planned programme
* Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
* Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
* Pupils should be helped to understand the need for pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
* Staff should act as good role models in their use of digital technologies the internet and mobile devices
* in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
* Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

**Technical - infrastructure / equipment, filtering and monitoring**

**The technical provision is through Conwy ICT team**

* They will be managed in ways that ensure that the school meets recommended technical requirements
* 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.
* Internet access is filtered for all users. Internet content is filtered by the Local Authority (CCBC ICT) through the use of a website filtering system to prevent the access of indecent and inappropriate internet content. The school is able to request websites be blocked and a website added to a content list if deemed inappropriate by a member of the SMT. Staff should report all websites deemed inappropriate to the Site lead/Head of PRU.
* Appropriate security measures are in place to protect the servers, firewalls, routers, wireless network, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. Firewalls are managed by the Local Authority (CCBC ICT), the physical location of servers and routers is controlled through lockable cabinets and, where possible, through locked designated rooms.
* Workstations are kept from the view of windows, where possible are covered and window blinds closed when the school is unoccupied. The schools wireless network is secured by WPA2 security and is only accessible by school and Local Authority devices. The school infrastructure and individual workstations are protected by up to date virus software.
* An agreed Acceptable Use policy is in place that details the expectation of staffs use of ICT devices, system and email addresses provided by and used within the school.

Unsuitable / inappropriate activities

It is required in all cases of unsuitable/inappropriate activities (as detailed below) that responsible staff report to the Head of PRU

Some internet activity is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

* Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978
* Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
* Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008
* criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986
* pornography
* promotion of any kind of discrimination
* threatening behaviour, including promotion of physical violence or mental harm
* any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
* Using school systems to run a private business
* Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
* Infringing copyright
* Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
* Creating or propagating computer viruses or other harmful files
* Unfair usage (downloading / uploading large files that hinders others in their use of the internet)
* On-line gaming (non educational)
* On-line gambling

**Responding to incidents of misuse**

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity report immediately to the Head of PRU.

**Other Incidents**

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

* Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
* Seek advice from HR
* Liaise with CCBC ICT
* Inform CCBC Safeguarding lead
* Record the URL (web address) of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
* Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
* Internal response or discipline procedures
* Involvement by Local Authority
* Police involvement and/or action
* If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
* incidents of ‘grooming’ behaviour
* the sending of obscene materials to a child
* adult material which potentially breaches the Obscene Publications Act
* criminally racist material
* other criminal conduct, activity or materials
* Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

**School Actions**

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

Revised:

* Spring Term 2019

Reviewed

* Autumn 2019
* Autumn 2021
* Autumn 2022

##### Rules for Responsible Internet Use

The schools have computers with Internet access to help our learning. These rules will keep you safe and help us be fair to others.

1. **I will only access the computer with permission from a member of staff**
2. **I will not access other people's files;**
3. **I will use the computers for school work and homework;**
4. **I will not bring in pen drives from outside school u**
5. **I will ask permission from a member of staff before using the Internet;**
6. **I will only E-mail people I know, or my teacher has approved;**
7. **The messages I send will be polite and responsible;**
8. **I will not give my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;**
9. **I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself;**
10. **I understand that the school may check my computer files and may monitor the Internet sites I visit.**

# Canolfan Addysg Conwy

### Acceptable Internet Use Statement

### For Staff and Students

The computer system is owned by the school, and may be used by staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties - the pupils, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff and students requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to the IT Manager for approval.

1. All Internet activity should be appropriate to staff professional activity or the student's education;
2. Access should only be made via the authorised account and password, which should not be made available to any other person;
3. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden;
4. Users are responsible for all E-mail sent and for contacts made that may result in E-mail being received;
5. Use for personal financial gain, gambling, political purposes or advertising is forbidden;
6. Copyright of materials must be respected;
7. Posting anonymous messages and forwarding chain letters is forbidden;
8. As E-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
9. Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.