



## Yr Athrofa E-Safety Policy

---

### Scope of the Policy

---

This policy applies to all members of Yr Athrofa community (including staff, students, volunteers, visitors, community users) who have access to and are users of Yr Athrofa ICT systems, within Yr Athrofa PLP setting.

### Background / Rationale

---

New technologies are integral to the lives of young people in today's society, both within primary, secondary schools, universities and in their lives outside of Yr Athrofa setting.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers / lecturers, students learn from each other. These technologies can stimulate discussion, promote creativity, collaboration and increase awareness of context to promote effective learning. Students should have an entitlement to safe internet access at all times.

The requirement to ensure that students are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all at Yr Athrofa are bound. Yr Athrofa e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in education from the head of Yr Athrofa, directors of discipline to heads of school, senior leaders, year leads, personal tutors, support staff, members of Yr Athrofa PLP and the students themselves.

The use of these exciting and innovative tools in the universities and at home has been shown to raise educational standards and promote trainee achievement.

However, the use of these new technologies can put students at risk within and outside the university. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming (e.g. victim of cat-fishing) by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other Yr Athrofa / University policies (e.g. behaviour, anti-bullying, Acceptable Use policies).

It is impossible to eliminate risks completely. Therefore, it is essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Yr Athrofa must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help students and young people to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

## Development / Monitoring / Review of this Policy

---

Consultation has taken place with the following key stakeholders:

- Head of Yr Athrofa
- Directors of discipline
- Senior Lecturers/Lecturers
- Lead and Network Schools
- Support Staff
- Information Services staff

Consultation has taken place through the following:

- Staff meetings
- University Lectures / Tutorials
- Yr Athrofa Trainee Forums
- Student Self Evaluation team
- Mentor Training Sessions
- Yr Athrofa website / newsletters

## Schedule for Development / Monitoring / Review

---

|                                                                                                                                                                                                                                                                          |                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| This e-safety policy was approved by the Management Board of Yr Athrofa PLP:                                                                                                                                                                                             | <i>TBC</i>                                          |
| The implementation of this e-safety policy will be monitored by the:                                                                                                                                                                                                     | <i>TBC</i>                                          |
| Monitoring will take place at regular intervals:                                                                                                                                                                                                                         | <i>Annually</i>                                     |
| The <i>Head of Yr Athrofa</i> will receive a report on the implementation of the e-safety policy generated by the e-safety co-ordinator in consultation with directors of disciplines (which will include anonymous details of e-safety incidents) at regular intervals: | <i>End of Semester 1<br/>End of semester 2</i>      |
| The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:                  | <i>TBC</i>                                          |
| Should serious e-safety incidents take place, the following external persons / agencies should be                                                                                                                                                                        | Dyfed Powys/South Wales Police and Student services |

The Athrofa PLP will monitor the impact of the policy using:

- Logs of reported incidents
- University monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of students, staff and partnership school

## Roles and Responsibilities

---

The following section outlines the roles and responsibilities for e-safety of individuals and groups within Yr Athrofa.

### Management Board of Yr Athrofa PLP

---

The Management Board of Yr Athrofa PLP are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Directors of discipline receiving regular information about e-safety incidents and monitoring reports.

The role of the Directors of discipline will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to Head of Yr Athrofa

### Directors of disciplines:

---

- Directors of disciplines are responsible for ensuring the safety (including e-safety) of members of Yr Athrofa community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- Directors of disciplines are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- Directors of disciplines will ensure that there is a system in place to allow for monitoring and support of those in Yr Athrofa 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.
- Directors of disciplines will receive regular monitoring reports from the E-Safety Co-ordinator.
- Directors of disciplines 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 or students.

### E-Safety Co-Ordinator:

---

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing Yr Athrofa e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with partnership ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,

- meets regularly with Directors of disciplines to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Directors of discipline

## Lecturing and Support Staff

---

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current Athrofa E-safety policy and practices
- they have read, understood and signed the University Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation / action / sanction
- digital communications with Students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official university systems
- e-safety issues are embedded in all aspects of the curriculum and other Yr Athrofa activities
- Students understand and follow the school e-safety and acceptable use policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lectures, extra curricular and extended Centre activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lectures where internet use is pre-planned Students 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
- are aware of the potential for serious protection issues to arise from, sharing of personal data, access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming and cyber-bullying

## Students:

---

- are responsible for using the University ICT systems in accordance with the University Acceptable Use Policy, which they will be expected to sign before being given access to university systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (Module Handbooks).
- 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 Centre policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand Centre 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 the university and realise that Yr Athrofa's E-Safety Policy covers their actions out of the university, if related to their membership of Yr Athrofa.

## Education – Students

---

Whilst regulation and technical solutions are very important, their use must be balanced by educating Students to take a responsible approach. The education of Students in e-safety is therefore an essential part of Yr Athrofa's e-safety provision. Students may require the help and support of Yr Athrofa to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety lecture will be provided as part of Undergraduate and Postgraduate programme - this will cover both the use of ICT and new technologies in the university and outside of the university
- Key e-safety messages should be reinforced as part of a planned programme of tutorial / pastoral activities
- Students should be taught in all sessions to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of ICT, the internet and mobile devices

## Education & Training – Staff

---

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand Yr Athrofa e-safety policy and University Acceptable Use Policies
- The E-Safety Coordinator will receive regular updates through attendance at regional and national training sessions and by reviewing guidance documents released by WG, NACE and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings.
- The E-Safety Co-ordinator will provide advice / guidance / training as required to individuals as required

## Curriculum

---

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

- in lectures where internet use is pre-planned, it is best practice that Students 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 Students are allowed to freely search the internet, e.g. using search engines, 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 may normally result in internet searches being blocked. In such a situation, staff can request that the Information Systems Manager (and other relevant person) 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.
- Students should be taught in all lectures if appropriate to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

## Use of digital and video images - Photographic, Video

---

The development of digital imaging technologies has created significant benefits to learning, allowing staff and Students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The

school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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 e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow university policies concerning the sharing, distribution and publication of those images. Those images should only be taken on university equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that Students are appropriately dressed and are not participating in activities that might bring the individuals or Yr Athrofa 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 without their written permission.
- Written permission from Students will be obtained before photographs of Students are published on Yr Athrofa website.
- Students work can only be published with the permission of the trainee.

## Data Protection

---

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018 which states that personal data must be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and, where necessary, kept up to date
- kept in a form which permits identification of data subjects for no longer than is necessary
- processed in a manner that ensures appropriate security of the personal data

Staff must 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, USB stick or any other removable media:

- the data must be encrypted and password protected or make use of biometric technology
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password / biometric protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with Yr Athrofa policy (below) once it has been transferred or its use is complete

## Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

| Communication Technologies                                              | Staff & other adults |                          |                            |             | Students |                          |                               |             |
|-------------------------------------------------------------------------|----------------------|--------------------------|----------------------------|-------------|----------|--------------------------|-------------------------------|-------------|
|                                                                         | Allowed              | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed  | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to university                              | ✓                    |                          |                            |             | ✓        |                          |                               |             |
| Use of mobile phones in lectures                                        | ✓                    |                          |                            |             |          | ✓                        |                               |             |
| Taking photos on mobile phones or other camera devices during lectures  | ✓                    |                          |                            |             |          | ✓                        |                               |             |
| Use of hand held devices e.g. Tablet computers                          | ✓                    |                          |                            |             |          | ✓                        |                               |             |
| Use of personal email addresses in university, or on university network | ✓                    |                          |                            |             | ✓        |                          |                               |             |
| Use of university email for personal emails                             | ✓                    |                          |                            |             |          |                          |                               | ✓           |
| Use of chat rooms / facilities                                          | ✓                    |                          |                            |             | ✓        |                          |                               |             |
| Use of instant messaging                                                | ✓                    |                          |                            |             | ✓        |                          |                               |             |
| Use of social networking sites                                          | ✓                    |                          |                            |             | ✓        |                          |                               |             |
| Use of blogs                                                            | ✓                    |                          |                            |             | ✓        |                          |                               |             |

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

- **The official Athrofa email service may be regarded as safe and secure and is monitored.** *Staff and Students should therefore use only the university email service to communicate with others when at university, or on university systems (eg by remote access).*
- **Users need to be aware that email communications may be monitored**
- **Users must immediately report, to the e-safety coordinator in the first instance – in accordance with the settings' policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.**

- **Any digital communication between staff and Students (email, chat, VLE etc) must be professional in tone and content.** These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- *Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

## Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images, distributing racist material or inciting forms of hatred is illegal and would obviously be banned from Athrofa or its Partnership and all other ICT 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 University context, either because of the age of the users or the nature of those activities.

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

### User Actions

|                                                                                                                                                                                       | Acceptable                                                                                                                                          | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|--------------------------------|--------------|--------------------------|
| <b>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:</b> | child sexual abuse images                                                                                                                           |                             |                                |              | ✓                        |
|                                                                                                                                                                                       | promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation                               |                             |                                |              | ✓                        |
|                                                                                                                                                                                       | adult material that potentially breaches the Obscene Publications Act in the UK                                                                     |                             |                                |              | ✓                        |
|                                                                                                                                                                                       | criminally racist material in UK                                                                                                                    |                             |                                |              | ✓                        |
|                                                                                                                                                                                       | pornography                                                                                                                                         |                             |                                | ✓            |                          |
|                                                                                                                                                                                       | Inappropriate sharing or transmitting of private/personal images/video e.g. "sex-ting"                                                              |                             |                                | ✓            |                          |
|                                                                                                                                                                                       | promotion of any kind of discrimination                                                                                                             |                             |                                | ✓            |                          |
|                                                                                                                                                                                       | promotion of racial or religious hatred                                                                                                             |                             |                                | ✓            |                          |
|                                                                                                                                                                                       | 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                                                                                                                                        |                                                                                                                                                     |                             |                                | ✓            |                          |
| Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions                       |                                                                                                                                                     |                             |                                | ✓            |                          |

|                                                                                                                                                                                    |   |   |  |   |  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|--|---|--|
| Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)                   |   |   |  | ✓ |  |
| Creating or propagating computer viruses or other harmful files                                                                                                                    |   |   |  | ✓ |  |
| Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet |   |   |  | ✓ |  |
| On-line gaming (educational)                                                                                                                                                       |   | ✓ |  |   |  |
| On-line gaming (non educational)                                                                                                                                                   |   |   |  | ✓ |  |
| On-line gambling                                                                                                                                                                   |   |   |  | ✓ |  |
| On-line shopping / commerce                                                                                                                                                        | ✓ |   |  |   |  |
| File sharing                                                                                                                                                                       |   | ✓ |  |   |  |
| Use of social networking sites                                                                                                                                                     |   | ✓ |  |   |  |
| Use of video broadcasting e.g. Youtube                                                                                                                                             | ✓ |   |  |   |  |

## Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

**If any apparent or actual misuse appears to involve illegal activity i.e.**

- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the Centre flow chart diagram should be followed.

It is more likely that the Centre 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 Centre community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

## Students

## Actions / Sanctions

| Incidents:                                 | Refer to tutor | Refer to Year Leads or Personal Tutors | Refer to Director of Discipline | Refer to E-Safety Coordinator | Refer to Police | Refer to technical support staff for action re filtering / security etc | Removal of network / internet access rights | Warning | Further sanction |
|--------------------------------------------|----------------|----------------------------------------|---------------------------------|-------------------------------|-----------------|-------------------------------------------------------------------------|---------------------------------------------|---------|------------------|
| Deliberately accessing or trying to access |                | ✓                                      | ✓                               | ✓                             | ✓               |                                                                         |                                             |         |                  |

|                                                                                                                          |   |   |   |   |   |   |   |   |   |
|--------------------------------------------------------------------------------------------------------------------------|---|---|---|---|---|---|---|---|---|
| <b>material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b> |   |   |   |   |   |   |   |   |   |
| Unauthorised use of non-educational sites during lessons                                                                 | ✓ |   |   | ✓ |   |   |   |   |   |
| Unauthorised use of mobile phone / digital camera / other handheld device                                                | ✓ |   |   | ✓ |   |   |   |   |   |
| Unauthorised use of social networking / instant messaging / personal email                                               | ✓ |   |   | ✓ |   |   |   |   |   |
| Unauthorised downloading or uploading of files                                                                           | ✓ | ✓ | ✓ | ✓ |   |   |   | ✓ |   |
| Allowing others to access school network by sharing username and passwords                                               | ✓ |   | ✓ | ✓ |   | ✓ |   |   |   |
| Attempting to access or accessing the school network, using another student's / pupil's account                          | ✓ | ✓ | ✓ | ✓ |   |   | ✓ |   |   |
| Attempting to access or accessing the school network, using the account of a member of staff                             |   |   | ✓ | ✓ |   |   | ✓ |   |   |
| Corrupting or destroying the data of other users                                                                         |   |   | ✓ | ✓ |   |   | ✓ |   | ✓ |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature              |   |   | ✓ | ✓ | ✓ |   | ✓ |   | ✓ |
| Continued infringements of the above, following previous warnings or sanctions                                           |   |   | ✓ | ✓ |   |   | ✓ |   | ✓ |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school                   |   |   |   | ✓ |   |   |   |   |   |
| Using proxy sites or other means to subvert the Centres filtering system                                                 |   |   |   | ✓ |   |   |   |   |   |
| Accidentally accessing offensive or pornographic material and failing to report the incident                             |   |   |   | ✓ |   |   |   |   | ✓ |
| Deliberately accessing or trying to access offensive or pornographic material                                            |   | ✓ | ✓ | ✓ |   |   |   |   | ✓ |
| Receipt or transmission of material that infringes the copyright of another person or infringes the GDPR                 | ✓ | ✓ | ✓ | ✓ |   |   |   |   |   |

## Staff Actions / Sanctions

|                                                                                                                                                                     |                                 |                             |             |                 |                                                              |         |            |                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-----------------------------|-------------|-----------------|--------------------------------------------------------------|---------|------------|---------------------|
| Incidents:                                                                                                                                                          | Refer To Director of Discipline | Refer to Head of Yr Athrofa | Refer to HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc | Warning | Suspension | Disciplinary action |
| <b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b> |                                 | ✓                           | ✓           | ✓               |                                                              |         |            |                     |
| Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email                                              | ✓                               |                             |             |                 |                                                              |         |            |                     |
| Unauthorised downloading or uploading of files                                                                                                                      |                                 | ✓                           | ✓           |                 |                                                              |         |            |                     |

|                                                                                                                                                                            |   |   |   |  |   |  |  |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|--|---|--|--|---|
| Allowing others to access University network by sharing username and passwords or attempting to access or accessing the university network, using another person's account |   |   | ✓ |  |   |  |  |   |
| Careless use of personal data e.g. holding or transferring data in an insecure manner                                                                                      | ✓ |   | ✓ |  |   |  |  |   |
| Deliberate actions to breach data protection or network security rules                                                                                                     |   |   | ✓ |  |   |  |  |   |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software                                                                      |   |   | ✓ |  |   |  |  |   |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature                                                                |   |   | ✓ |  |   |  |  |   |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with Student teachers                                 | ✓ |   |   |  |   |  |  |   |
| Actions which could compromise the staff member's professional standing                                                                                                    |   |   | ✓ |  |   |  |  |   |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school                                                                     | ✓ | ✓ | ✓ |  |   |  |  |   |
| Using proxy sites or other means to subvert the school's filtering system                                                                                                  |   |   | ✓ |  | ✓ |  |  |   |
| Accidentally accessing offensive or pornographic material and failing to report the incident                                                                               | ✓ | ✓ | ✓ |  |   |  |  |   |
| Deliberately accessing or trying to access offensive or pornographic material                                                                                              | ✓ | ✓ | ✓ |  |   |  |  |   |
| Breaching copyright or licensing regulations                                                                                                                               |   | ✓ | ✓ |  |   |  |  |   |
| Continued infringements of the above, following previous warnings or sanctions                                                                                             |   |   | ✓ |  |   |  |  | ✓ |

Date on which policy was approved: .....

Policy review date: .....

## Acknowledgements

SWWCTE would like to acknowledge a range of individuals and organisations whose policies; documents, advice and guidance have contributed to the development of this Centre E-Safety Policy:

- South West Grid for Learning
- Becta
- National Education Network (NEN)
- London Grid for Learning
- Kent County Council (Schools and Settings E-safety Policy Guidance)
- Edge Hill University
- <http://www.childreninwales.org.uk>
- JISC

- Byron Review – Children and New Technology – “Safer Children in a Digital World”

## **See below for a summary of the main points from relevant Parliamentary Acts Relating to Yr AthrofaE-Safety Policy**

### **Copyright, Designs and Patents Act 1988**

---

This Act, together with a number of Statutory Instruments that have amended and extended it, controls copyright law. It makes it an offence to copy all, or a substantial part, which can be a quite small portion, of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, sound, moving images, TV broadcasts and many other media.

### **Malicious Communications Act 1988**

---

Under this Act it is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person. Additionally under the Telecommunications Act 1984 it is a similar offence to send a telephone message, which is indecent, offensive, or threatening.

### **Computer Misuse Act 1990**

---

This Act makes it an offence

- to erase or amend data or programs without authority;
- to obtain unauthorised access to a computer;
- to "eavesdrop" on a computer;
- to make unauthorised use of computer time or facilities;
- maliciously to corrupt or erase data or programs;
- to deny access to authorised users.

### **Criminal Justice & Public Order Act 1994**

---

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:-

- use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- display any writing, sign or other visible representation which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

### **Trade Marks Act 1994**

---

This Act provides protection for Registered Trade Marks, which can be any symbol (words or images) or even shapes of objects that are associated with a particular set of goods or services. Anyone who uses a Registered Trade Mark without permission can expose themselves to litigation. This can also arise from the use of a Mark that is confusingly similar to an existing Mark.

### **Data Protection Act 1998**

---

The University has a comprehensive [Data Protection Policy](#), of which the following statement is the summary.

## **Human Rights Act 1998**

---

This act does not set out to deal with any particular mischief or address specifically any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the context of the University, important human rights to be aware of include:

- the right to a fair trial
- the right to respect for private and family life, home and correspondence
- freedom of thought, conscience and religion
- freedom of expression
- freedom of assembly
- prohibition of discrimination
- the right to education

These rights are not absolute. The University, together with all users of its IT services, is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations which arise from other relevant legislation.

## **Regulation of Investigatory Powers Act 2000**

---

The Act states that it is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic (including telephone) communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.

Monitoring but not recording is also permissible in order to:

- Ascertain whether the communication is business or personal;
- Protect or support help line staff.

The University reserves the right to monitor e-mail, telephone, and any other communications in line with its rights under this act. The Lawful Business Practice Regulations allow exceptions to the basic principle of non interception as stated in the RIPA, and allows interception without consent in certain instances.

## **Freedom of Information Act 2000**

---

The Act, intended to increase openness and transparency, obliges public bodies, including Higher Education Institutions, to disclose a wide range of information, both proactively and in response to requests from the public. The types of information that may be have to be found and released are wide-ranging, for example minutes recorded at a board meeting of the institution or documentation relating to important resolutions passed. Retrieval of such a range of information places a considerable burden on an institution subject to such an information request. In addition to setting a new standard of how such bodies disseminate information relating to internal affairs, the Act sets time limits by which the information requested must be made available, and confers clearly stated rights on the public, regarding such information retrieval. Therefore all staff have a responsibility to know what information they hold and where and how to locate it. The University has adopted a comprehensive publication scheme.

## **Communications Act 2003**

---

This act makes it illegal to dishonestly obtain electronic communication services, such as e-mail and the World Wide Web.

### **Criminal Justice and Immigration Act 2008**

---

This act increased the penalties for publishing an obscene article. It also introduced fines for data protection contraventions when organisations 'knew or ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial distress or damage, but failed to take reasonable steps to prevent the contravention.

### **General Data Protection Regulation 2018**

---

The University has a comprehensive Data Protection Policy, of which the following statement is the summary.

DRAFT