# E-SAFETY POLICY

*Academic Year*
*2026 - 2027*

# E-Safety Policy

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, and community users) who have access to and use digital systems inside and outside the school). It also applies to the use of personal digital technology on school premises (where permitted).

## Develop / monitor / review this policy

This online security policy has been developed by an ICT working group which includes:

- *Head/senior leaders*
- *Online safety officer/coordinator*
- *Staff - including practitioners, support staff, technical staff*
- *Governors*
- *Parents and carers*
- *Community users.*

The whole school/college community was consulted at a variety of formal and informal meetings.

### Timetable for development / monitoring / review

| | |
|---|---|
| This online safety policy was approved by the governing body */ sub-committee of governors on:* | *10/10/24* |
| The following will monitor the implementation of this online safety policy: | *Headteacher* |
| Monitoring will take place on a regular basis: | *Annually* |
| The *governing body / sub-committee of governors will receive* a report on the implementation of the online safety policy which will be produced by the monitoring group (it will include anonymised details of online security cases) on a regular basis: | *Annually* |
| The online security policy will be reviewed annually, or more frequently in light of significant new developments in the use of technologies, new threats to online security or any incidents that have occurred. It is anticipated that the next review date will be on: | |
| In the event of serious online security incidents, these external persons / agencies should be informed that: | *LA ICT Manager, LA Security Officer, Police – relying on the incident.* |

The school will monitor the impact of the policy by:

- *Recording incidents*
- *Monitoring records of internet activity (including the websites that have been used)*

- *Keep internal data monitoring network activities*
- *Conduct surveys or questionnaires for:*
    - *Learners*
    - *parents and carers*
    - *staff.*

- We believe we have a duty to provide pupils with quality Internet access as part of their learning experience across all curricular areas. The use of the Internet is an invaluable tool in the development of lifelong learning skills.

We believe that used correctly Internet access will not only raise standards, but it will support teacher's professional work and it will enhance the school's management information and business administration systems

We acknowledge that the increased provision of the Internet in and out of school brings with it the need to ensure that learners are safe. We need to teach pupils how to evaluate Internet information and to take care of their own safety and security.

E-Safety, which encompasses Internet technologies and electronic communications, will educate pupils about the benefits and risks of using technology and provides safeguards and awareness to enable them to control their online experience.

We believe all pupils and other members of the school community have an entitlement to safe Internet access at all times.

We have a duty to safeguard children, young people and families from violent extremism. We are aware that there are extremists groups within our country who wish to radicalise vulnerable children and to involve them in terrorism or in activity in support of terrorism. Periodic risk assessments are undertaken to assess the risk of pupils being drawn into terrorism. School personnel must be aware of the increased risk of online radicalisation, and alert to changes in pupil's behaviour. Any concerns will be reported to the Designated Safeguarding Lead.

We are aware that under the 'Counter-Terrorism and Security Act 2015' we have the duty to have 'due regard to the need to prevent people from being drawn into terrorism'. This duty is known as the Prevent duty and we believe it is essential that school personnel are able to identify those who may be vulnerable to radicalisation or being influenced by extremist views, and then to know what to do when they are identified.

We provide a safe environment where we promote pupils' welfare. Within this environment we work hard to build pupils' resilience to radicalisation and extremism by promoting fundamental British values and for everyone to understand the risks associated with terrorism. We want pupils to develop their knowledge and skills in order to challenge extremist views.

We wish to work closely with the School Council and to hear their views and opinions as we acknowledge and support Article 12 of the United Nations Convention on the Rights of the Child that children should be encouraged to form and to express their views.

We as a school community have a commitment to promote equality. Therefore, an equality impact assessment has been undertaken and we believe this policy is in line with the Equality Act 2010.

We believe it is essential that this policy clearly identifies and outlines the roles and responsibilities of all those involved in the procedures and arrangements that is connected with this policy.

# Roles and responsibilities

The following section outlines the roles and responsibilities of individuals and groups within the school related to online safety:[1]

## Governors

The Governors are responsible for approving the online safety policy and for reviewing the effectiveness of the policy. This will be achieved by the *Governing Body / governors' sub-committee.* They receive regular information and monitoring reports in relation to online safety incidents. A member of the Governing Body should take on the role of online safety governor and:[2]

- meet regularly with the online co-ordinator / security officer
- regularly monitor records of online safety incidents
- regular monitoring of records governing filter switching and monitoring of filter records (where possible)
- report to the relevant governors / sub-committee / meeting.

## Headteachers and senior leaders

- It is the headteacher's duty to ensure the safety (including online safety) of all members of the school/college community. However, the online security coordinator/officer is allowed to assume daily responsibilities for online safety.
- The headteacher and (at least) one other member of the senior management team should be aware of the procedures that need to be followed in the event of a serious allegation relating to online safety against a member ofstaff.[3]
- The headteacher/senior leaders are responsible for ensuring that the online safety coordinator/officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to provide training to co-workers where relevant.
- The headteacher/senior leaders will ensure that a system is in place to be able to monitor and provide support to those monitoring the school's internal online safety. This will safeguard and support the workers who are addressing important monitoring roles.
- The headteacher/senior leaders will receive regular monitoring reports from the staff re: any concerns and from LA Officers.

## Online co-ordinator / security officer – Daniel Lewis

The online security co-ordinator / officer will:

- lead the online safety committee
- take responsibility for reporting online safety issues
- ensure that all staff are aware of the procedures that should be followed in cases of online safety incidents.
- provide training and advice to staff (or identify appropriate sources of that)
- contact the relevant local authority/body
- liaising with technical staff – iteach / CARDIFF ICT

---

[2] It is suggested that this role be combined with that of the Safeguarding Governor

[3] See flowchart for dealing with online security incidents- which is included in a section later - "Responding to abuses" and disciplinary procedures *Local Authority Human Resources / other relevant body*

- receive reports on online safety incidents and create a record of events to be used to develop future online safety[4]
- meet regularly with the online safety governor to discuss current issues and review event logs
- attend relevant governors' meetings/sub-committees
- report consistently to the headteacher

## Network manager /technical staff: i-teach / Cardiff ICT

The network manager / technical staff (or managed service provider/local authority) are responsible for ensuring that:

- that the school's technical infrastructure is safe and cannot be misused or subjected to *malicious attacks*
- the school/college meets (at a minimum) the necessary online safety technical requirements identified by *the*local authority or other relevant*body,* as well as the online safety policy/guide that may apply
- users will only have access to the network and devices through a properly enforced password protection policy and where the passwords are constantly being changed
- they are aware of the latest technical information on online safety to carry out the online safety role effectively and to keep others informed of updates where relevant
- the use of the *network/internet/learning platform/Hwb/remote access/e-mail is constantly* monitored so that any misuse or attempt to misuse the systems can be reported to the *headteacher/senior leader; coordinator/online security officer* so that any misuse or attempt to misuse the systems can be reported to the headteacher/action/prevention
- *that monitoring software/systems (if any exist) are implemented and updated as agreed in the school's policies*
    - *that the filtering policy (*if one exists*) is implemented and updated consistently and that its implementation is not the sole responsibility of one person*

## Learning and Support Staff

These individuals are responsible for ensuring that:

- current awareness of online safety issues and of the school's current online safety policy and practices
- they have read, understood and signed the staff acceptable use agreement (CDD)
- that they inform the *headteacher/senior leader; an online security coordinator/officer of* any misuse or problem, so that he/she can investigate/act
- that all digital communication with learners/parents and carers is carried out at a professional *level and when using the official school/college systems only*
- that online safety issues are an integral part of all aspects of the curriculum and other activities
- that learners understand and follow the online safety and acceptable use agreements
- that learners have a good understanding of research skills and of the need to avoid plagiarism and adhere to copyright rules
- that they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school/college activities (where permitted) and implement up-to-date policies relating to these devices
- in lessons where internet use is planned, learners should be directed to websites that have been checked as suitable for use, *and that a process is in place to deal with any unsuitable* material discovered when searching the internet

[4] The school/college will need to decide how they will respond to these incidents and whether the investigation/action is the responsibility of the online coordinator/safety officer or other member of staff e.g. headteacher/senior leader/designated senior person/class teacher/head of year etc

## Online safety group

The online safety group is an advisory group made up of wide representation from the school community. It is responsible for online safety issues and monitoring of the online safety policy, including the impact of the schemes. Depending on the size or structure of the school/college, this committee may be part of the safeguarding group. The group will also be responsible for reporting regularly to senior leaders and the governing body.[5]

Members of the online security group (or other relevant group) will assist the online security coordinator/officer (or other relevant person as noted above) with the following:

- production/review/monitoring of school/college online safety policy/documents
- *produce/review/monitor the school/college filtering policy (if possible and if the school/college chooses to have one) and request filtering changes*
- mapping and reviewing online safety education provision - ensuring relevance, breadth and progression
- monitor the network/internet/event logs where possible
- consultation with stakeholders – including parents/carers and learners on online safety provisions
- monitor the improvement actions identified using the 360 degree safe Wales self-review tool

An online safety group remit template can be found in the appendices.

## Learners

- these individuals are responsible for using the school's digital technologies systems in accordance with the acceptable use agreement for learners (this should include personal devices – where permitted)
- they should have a good understanding of research skills and the need to avoid plagiarism and adhere to copyright rules
- they must understand the importance of reporting abuse, misuse or access to inappropriate material, and know how to do so
- they are expected to be aware of and understand the policies on the use of mobile devices and digital cameras. They should also understand and be aware of policies relating to taking and using photographs, and to online bullying
- they must understand the importance of following good online safety practices when using digital technologies outside school and realise that the school/college's online safety policy applies outside of school/college if it relates to school membership

## Parents and carers

Parents and carers have a vital role to play in ensuring that children understand the need to use the internet/mobile devices appropriately. The school will take every opportunity to help parents and carers understand these issues by holding *parent/carer evenings, newsletters, letters, websites, Hwb, learning platforms and information about national/local online safety campaigns/literature.* The school/college will encourage parents and carers to support them by promoting good online safety practices and following the guidance on appropriate use of:

- digital images and videos taken at school events
- access to sections of the website for parents/carers, Hwb, learning platforms and learners' online records
- their children's personal devices at school (where they may be used)

### Community users

Community users who have access to the school/college's systems/website/Hwb/learning platform as part of the wider school/college provision, will be expected to sign an acceptable community user use agreement before accessing the school/college systems.

# Policy statements

## Education - learners

Although regulations and technical solutions are very important, their use must be balanced with teaching learners to take a responsible approach. Educating learners about online safety is therefore an essential part of the school/college's online safety provision. Learners need the help and support of the school/college to identify online safety risks, avoid them and build their resilience.

The focus should be on online safety across the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant, provide continuity, and provide opportunities for creative activities that will be delivered in the following ways.

- **An online safety curriculum designed across a range of subjects and subject areas should often be revisited.**
- **Essential online safety messages should be reinforced as part of a planned morning services and tutorial/pastoral activities program.**
- **Learners in all lessons should be taught to be very aware of the material/content they access online and encourage them to validate the accuracy of information.**
- **All learners should be taught to recognise the source of the information used and to respect copyright when using material accessed on the internet.**
- Learners should be helped to combat radicalisation by providing a safe environment to discuss controversial issues and helping them to understand how they can influence and participate in decisions. Nb. there are additional duties for schools/colleges under the Counter Terrorism and Security Act 2015, which requires schools/colleges to ensure that children are safe from terrorist and extremist materials on the internet.
- *Learners should be helped to understand the need for an acceptable learner use agreement and encouraged to adopt safe and responsible use in and outside school/college.*
- *Staff should set a good example of using digital technologies, the internet and mobile devices.*
- *Where lessons have been planned to use the internet, best practice would be to refer learners to verified websites so that they are suitable for use and that a process is in place to deal with any unsuitable material they encounter when searching the internet.*
- *When learners have freedom to access the internet, staff should be vigilant in monitoring the content of the websites visited by the young people.*
- *For educational reasons, it must be accepted from time to time that learners need to investigate subjects that are usually prohibited when using the internet (e.g. racism, drugs, discrimination). In such a situation, staff may ask technical staff (or another nominated person) to remove these exclusions from the filter list over the study period. Any request to do this should be able to be examined, and clear reasons for the need to do so.*

## Education - parents and carers

Many parents and carers have only a very limited understanding of online safety risks and issues, but play a vital role in their children's education and in monitoring/regulating their children's behaviour online. It is likely that parents do not realise how often children and young people come across inappropriate and harmful material online, and are not sure how to respond.

Therefore, the school will seek to provide information to parents and carers and raise their awareness by:

- *curriculum activities*
- *letters, newsletters, website, learning platform, Hwb*
- *evenings/sessions for parents and carers*
- *prominent events/campaigns e.g. Safer Internet Day*
- *refer to the relevant websites/publications e.g. hwb.wales.gov.uk www.saferinternet.org.uk/ www.childnet.com/parents-and-carers*

## Education - the wider community

The school/college will provide opportunities for local community groups/community members to benefit from the school/college's online safety information and experience. This will be offered in a number of ways:

- provide courses for families to learn to use new digital technologies, digital literacy and online safety
- online safety messages targeting grandparents and other relatives, as well as parents.
- the school's learning platform, Hwb, website, will provide online safety information to the wider community

## Education and training - staff / volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. The following training will be offered:

**a formal and planned online safety training programme will be available to staff which will be constantly updated and strengthened. An audit of the online safety training needs of all staff is carried out on a regular basis.** *It is expected that some staff will identify online safety training needs under the performance management process*

- **all new staff should receive online safety training as part of the induction programme to ensure that they fully understand the school/college's online safety policy and acceptable use agreements.**
- *the online security co-ordinator/officer (or other appointed person) will be kept informed by attending external training events (e.g. Consortium/SWGfL/LA/other relevant organisations) and by reviewing documents offering guidance from other relevant organisations.*
- *the online safety policy and updates to it, will be presented to staff for discussion at staff/team meetings or INSET days.*
- *the online security coordinator / officer (or other appointed person) will provide advice/guidance/training to individuals as required.*

## Training - Governors

**Governors should participate in online safety training/awareness sessions,** particularly those who are members of any subcommittee/group involved in technology/online safety/health and safety/safeguarding. This can be offered in a number of ways:

- attend training provided by the local authority/National Association of Governors /or other relevant organisation (e.g. SWGfL).
- participate in school/college training/information sessions for staff or parents

## Technical - infrastructure/equipment, filtering and monitoring

If the school/college has a managed ICT service provided by an external contractor, it is the responsibility of the school/college to ensure that the managed service provider performs all the online safety measurements that would otherwise be the responsibility of the school/college, as suggested below. It is also important that the managed service provider is fully aware of the school/college's online safety policy/acceptable use agreements.

The school/college should also check the policies of the Local Authority/other relevant body on these technical matters if the service is not provided by the Authority.

The school will be responsible for ensuring that the school/college infrastructure/ network is as safe as reasonably possible and that the policies and procedures approved in this policy are implemented. It will also be necessary to ensure that the relevant people named in the above sections carry out their online safety responsibilities effectively:

- **The school's technical systems will be managed in ways that ensure that the school meets the technical requirements suggested**
- The safety of the school/college's technical systems will be kept under constant review and audit.
- Servers, wireless systems and cables must be securely located and physical access to them restricted.
- There requires a robust back-up regime, which is validated for good practice in preventing data loss as a result of an attack by oyster software. This includes keeping copies off-site.
- **All school networks and systems will be protected by secure passwords.**
- **The passwords of the school's main systems accounts should be kept in a safe place e.g. in the school's memory. Consideration should also be given to using a two-factor authentication approach for such accounts The rights of access of all users to school/college technical systems and devices will be clearly defined. The Network Manager (or other individual) will record details of the access rights available to user groups. These will be reviewed** by the online security group (or other **group) at least once a year.**
- **All users (adults and learners) are responsible for the security of their username and password. They should not allow any other user to access the systems with their login details. They must report immediately if they suspect or if there is evidence that security has been undermined.**
- **Passwords should not be shared with anyone.**
- Mrs Huws ( DigitalLeader)will provide everyone with **a username and password,** and will keep an up-to-date record of users and their username (see the password creation section of the 'technical security policy template' in the Annex).
- **Passwords should be long. Good practice indicates that passwords containing over 12 characters are more difficult to resolve. Passwords containing over 16 characters and containing a combination of unrelated words are particularly difficult to resolve. Passwords should be easy to remember, but difficult to guess or solve.**
- **A record of learners' usernames and passwords in the Foundation Phase can be kept in electronic or paper format, but they must be kept securely when the user does not need them.** *Passwords should not be as complex for the foundation phase (for example, at least 6 characters) and should not contain special characters. The use of random words or sentences should be encouraged when external systems have different password requirements.*
- Requirements for key stage 2 and above learner passwords should increase as learners progress through school/college.
- **All users** (KS2 and above) will be given a secure username and password by the Digital Leader, who will keep an up-to-date record of the users and their usernames. Users are responsible for protecting their username and password. **The HWB password follows the child through school.**
- **The "main" passwords, or "administrator" passwords for the school/college digital systems used by the network manager (or other person), must also be made available to the principal or other appointed senior leader, and be kept in a secure place (e.g. school/college safe)**
- TheSchool 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 with the number of software settings

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband provider or filtered using the Internet Watch Foundation's CAIC list. The contents of the lists are regularly updated and internet use is regularly logged and monitored. A clear process is implemented that deals with requests for filter changes
- *Where possible, the school will provide improved/differentiated filters* at user level with the *assistance of the County and i-teach*
- Internet filtering should ensure that children are safe from terrorist and extremist material when using the internet.
- Where possible, school/college technical staff regularly monitor and record users' activities on school/college technical systems and users are informed of this in the acceptable use agreement
- There is an appropriate system in place – record an incident and provide the Digital Lead with users to report any actual or potential breaches of online security rules to the appropriate person, as agreed.
- Security measures are in place ( toprotectthe servers, guard walls, routers, wireless systems, workstations, mobile devices etc. from any accidental or malicious attempt that could threaten the safety of the school's systems and data.. The school's individual infrastructure and workstations are protected by current virus software.
- A policy is being implemented (to be described) which allows or prohibits staff from downloading executable files and installing programmes on school/college devices.

A policy is being implemented concerning the use of mobile media (e.g. memory small/CDs/DVDs) by users on school/college devices.

Personal data cannot be sent over the internet or removed from the school website if it is not securely encrypted or protected in another way e.g. sharinga privacy setting or saying who has access to thework.

## Mobile technologies

Mobile technology devices may be owned by the school/college or provided by the school/college or be personal property. It can include: a smartphone, tablet, notebook/laptop or other technology that can usually use the school's wireless network. The device then has access to the wider internet, which may include the school/college learning platform and other cloud-based services, such as e-mail and data storage.

All users should understand that the main purpose of using mobile/personal devices in a school context is educational purpose. The mobile technologies policy should be consistent and interconnected with, but not limited to, other relevant school/college policies – safeguarding, behaviour, anti-bullying, acceptable use, and relevant policies to steal or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be included as part of the school/college's online safety educational programme.

When preparing a mobile technologies policy, the school/college should consider the potential problems and risks. These include:

- security risks in allowing contact with your school network
- filter personal devices
- equipment cutting and insurance
- access to devices for all learners
- avoid possible disruption to the classroom
- network connection speed, device types
- charging facilities
- total cost of ownership.

It is possible to implement a range of mobile technologies.

I gael rhagor o wybodaeth, darllenwch *NEN Technical Strategy Guidance Note 5 – Bring your own device* - /www.nen.gov.uk/bring-your-own-device-byod/

- The school/college's acceptable use agreements for staff, learners, parents and carers, will take account of the use of mobile technologies.
- The school/college allows the following: (the school/college should complete the table below to indicate which devices are allowed and to define their access to the school/college systems)

| | School devices | | | Personal devices | | |
|---|---|---|---|---|---|---|
| | School property for an individual user | School premises for a number of users | Authorised device[6] | Student's property | Staff property | Staff property |
| Allowed at school | Device from iteach or Cardiff County | Device from iteach or Cardiff County | Device from iteach or Cardiff County | Need to give the class teacher a mobile phone in year 6, this is the year that tends to walk home. | To use for personal things during playtime/lunch not in class.<br><br>To use on an emergency school trip<br><br>Residential Course | With permission, a teacher can keep a stick on to receive urgent messages e.g. a phone call from the doctor<br><br>To use on an emergency school trip<br><br>Presswyl Course. |
| Full network access | Ie | Ie | Ie | Na | Ie - Public | Ie - Public |
| Internet only | | | | | | |
| No network access | | | | Na | As Above | As Above |

**Devices owned/provided by the school:**

- Who they will be distributed to.
- Where, when and how they may be used – times/places/in or out of school/college.

[6]Authorised device - purchased by the learner/family through a scheme organised by the school/college. This device can be given full network access, as if it were owned by the school/college.

- Whether personal use is permitted.
- Levels of access to the networks/internet (see above).
- Manage devices/install apps/change settings/monitor.
- Network/broadband capacity.
- Technical assistance.
- Hidlo dyfeisiau.
- Access to cloud services.
- Data protection.
- Remove/store/use images.
- Exit processes, what happens to stored devices/software/apps/data if the user leaves school/college.
- Liability for damage.
- Training for staff.

**Personal devices**

- Which users are allowed to use personal mobile devices in the school (staff/learners/visitors).
- Restrictions on where, when and how they can be used in school/college.
- Thick.
- Whether staff will be allowed to use personal devices for school matters.
- Levels of access to the networks/internet (see above).
- Network/internet capacity.
- Technical assistance (this may be a clear statement that technical assistance is not available).
- Filter the internet connection for these devices.
- Data protection.
- Remove/store/use images.
- Liability for loss/damage or malfunctioning following network access (likely to be a disclaimer regarding school/college responsibilities).
- Identification/labelling of personal devices.
- How to inform visitors of school/college requirements.
- How education about the safe and responsible use of mobile devices will be included in the school/college's online safety educational programme.

## Use digital and video images

The development of digital imaging technologies has generated significant benefits in teaching. It allows staff and learners to be able to use images they have recorded themselves, or downloaded from the internet, immediately. However, staff, parents, carers and learners need to be aware of the dangers associated with publishing digital images on the internet. Such images can lead to online ovulation cases. Digital images can remain on the internet forever and can cause harm or shame to individuals in the short or long term. It is common for employers to check the internet for information about potential or existing employees. The school/college will inform and educate users about these hazards and implement policies to reduce the likelihood of potential harm:

- **When using digital images, staff should inform and educate learners about the dangers associated with removing, using, sharing, publishing and distributing images. In particular, they should identify the risks associated with publishing their own images on the internet e.g. on social networking websites.**
- In line with guidance from the Information Commissioner's Office, parents/carers are welcome to take digital videos and images of their children at school events for personal use (as such use is not mentioned in the Data Protection Act). To respect everyone's privacy, and in some cases for safety, they should not be published/made public on social networking websites, and parents/carers should not comment on any activities involving *other* learners in the digital/video images.
- *Staff and volunteers have the right to take digital/video photographs to support educational aims, but the school's policies regarding the sharing, distribution and publication of these images must be followed. These images should only be taken on school/college equipment, and staff personal equipment should not be used for such a purpose.*
- *Care should be taken when taking digital/video images that learners are suit appropriately dressed and do not take part in activities that can bring the individual or school/college into disrepute.*
- *Learners should not remove, use, share, publish or distribute images of others without permission.*
- *Photographs involving learners published on the website or elsewhere will be carefully selected and conform to good practice guidance when using such images.*
- *The full names of learners are not used on websites or on blogs, particularly those linked to pictures.*
- *Written parental permission will need to be obtained before learners' pictures are published on the* school *website* or *on tweets*
- *A learner's work can only be published with the permission of learners and parents or carers.*

## Data protection

Personal data will be recorded, processed, transferred and released in accordance with existing data protection legislation.

The school must make sure that:

- **have a Data Protection Policy. (check the appendix for a model policy)**
- **that they implement the data protection principles and are able to demonstrate that they are doing so through the use of policies, notices and records.**
- **they have paid the appropriate fee to the Information Commissioner's Office and have included details of the Data Protection Officer.**
- **they have appointed an appropriate Data Protection Officer who has a high level of understanding of data protection law, and is free from conflict of interest.** The school/college may also wish to appoint a Data Controller and Systems Controller to assist the Data Protection Officer.
- **have an 'information asset register' in place and know exactly what personal data the register keeps, where and why the data is held, and which member of staff is responsible for managing the register**

- **the information asset register records the legal basis for processing personal data (including, where relevant, how consent was obtained, and how the consent was renewed). When data in a particular category is processed, the additional legal basis will also be recorded**
- **The register only retains the minimum amount of personal data appropriate to the performance of its function, and ensures that they do not keep the data for longer than is necessary for the purposes for which it was collected. The educational institution should develop and implement a 'data retention policy' to ensure that there are clear and understandable policies and practices in terms of deleting and removing data to support this. The personal data held must be accurate and up to date where this is necessary for the purposes for which the data is being processed. They must make sure they have systems in place to identify errors, such as asking parents to check emergency contact details at appropriate times**
- they provide staff, parents, volunteers, young people and older children with the information about how the school looks after their data and rights in a clear Privacy Notice (see the Privacy Notice section of the appendix)
- **that procedures are in place to deal with the individual rights of the data subject, e.g. one of the relevant data subject rights is Access to Data by the Person, which enables an individual to see a copy of the personal data held about them (subject to certain exceptions that may apply).**
- **that Data Protection Impact Assessments are carried out where necessary. For example, to make sure that personal data is protected when people use any remote access solutions, or enter into a relationship with a new supplier (also, it may be necessary to make sure that data processing clauses are included in the supplier's contract, or as an attachment)**
- that the IT system is secure and checked regularly. Patches and other essential safeguarding updates are put in place immediately to protect the personal data on the systems. They should make sure that there are administrative systems separate from the systems available in the classroom/for learners
- **that they have undertaken a proper due diligence process and have placed data processing clauses in contracts with any data processors who process personal data.**
- **that they understand how to share data with other relevant data controllers legally and securely. Schools in Wales should consider using the Wales Personal** Information Sharing Agreement **toolkit to help share data regularly between data controllers.**
- **they report any relevant offence to the** Information Commissioner within **72 hours of becoming aware of it, in accordance with UK data protection law. They should make sure that they report relevant cases of un authorised access to the individuals affected by this in accordance with the law. In order to do this, they will need to make sure that they have a policy for reporting, recording, managing, investigating and learning from information risk incidents.**
- **If it is a maintained school, they must have a Freedom of Information Policy setting out how they will deal with Freedom of Information requests.**
- **all staff receive data protection training during induction and receive appropriate refresher training thereafter. They should also ensure that staff undertaking data protection functions, such as dealing with requests under the individual's rights, receive appropriate training for their role together with the core training provided to all staff.**

When personal data is stored on any removable mobile device or media:

- **the data must be encrypted and password protected**
- **the device must be password protected.**

- **the device must be protected through current virus and malware checking software**
- **data must be securely deleted from the device, in accordance with school/college policy (below) after transmission or after completion of use.**

**Staff must:**

- **always be careful to make sure that personal data is kept securely, reducing the risk of losing or misusing the data**
- **identify a possible case of unincorporation of data, understand the need to hurry, and know to whom in school they should report such a case**
- **make sure they can help the data subject understand their rights and know how to deal with a request orally or in writing. It will need to know to whom this should be referred to in school**
- **They must also know where personal data is held or transmitted on mobile or other devices (including USBs). These must be encrypted and password protected.**
- **make sure they do not transfer any school/college personal data to personal devices if it is not in line with school policy**
- **make sure they only use records and personal data sources on computers or other password-protected secure devices, making sure they have logged out correctly at the end of any session where they use personal data**

## Communication technologies

Communication is a subject where technologies and their use develop very quickly. Schools/colleges will need to discuss and agree how they intend to implement and use these technologies, e.g. some schools/colleges allow learners to use mobile phones in lessons, while others see and allow educational benefits from their use. This section can also be influenced by the age of learners. The table has been kept blank so that schools/colleges can choose their own response.

It is possible for the wide range of communication technologies that are developing very quickly to improve teaching. The following table shows how the school/college considers whether the advantages of using these technologies for teaching outweigh the risks/disadvantages.

| Staff ac<br>Adults<br>Other | Learners |
|---|---|

| Communication Technologies | May | Permitted at certain times | Specific staff are allowed to | It is not permitted | May | Permitted at certain times | mitted with the permission of staff | It is not permitted |
|---|---|---|---|---|---|---|---|---|
| Bringing mobile phones to school/college | X | | | | | | X | |
| Use of mobile phones in lessons | | X | | X | | | | |
| Use of mobile phones in social periods | X | | | X | | | | |
| Taking pictures on mobile phones / cameras | | | X | | | | | |
| Use of other mobile devices e.g. tablets, gaming devices – SOME SCHOOL | X | | | x | | | | |
| Use personal e-mail addresses at school/college, or on the school/college network | | x | | x | | | | |
| Use school/college email for personal emails | x | | | | x | | | |
| Use messaging apps | | | x | X | | | | |
| Using social media | | | x | x | | | | |
| Use blogs | | | x | | | | x | |

The school/college may also wish to add some of the following policy statements relating to the use of communication technologies, rather than, or in addition to, the above table:

When using communication technologies, the school/college considers the following practices as examples of good ones:

- **the school's official e-mail service can be considered secure and is being monitored. Users should be aware that e-mail communications are being monitored.** *Therefore, learners should only use the school's e-mail service to communicate* with others in school or on the school systems (e.g. remote access).
- **in line with school/college policy, learners should inform the nominated person immediately if they receive any message that makes them feel uncomfortable, if the nature of the message is offensive, discriminatory, threatening, or bullying. Such messages should not be answered**
- **any digital communication between staff and learners or parents/carers (e-mail, chat, learning platform etc) must be professional in tone and content.** *This type of communication is permitted only on the official systems of the school (which are monitored). Personal email addresses, text messages and social media should not be used for this type of communication*
- *learners should be taught about online safety issues, such as the dangers associated with sharing personal details. They should also be taught about strategies about how to deal with inappropriate communications, and reminded of the need to communicate appropriately when using digital technologies.*

- *personal information should not be posted on the school/college website and only official e-mail addresses should be used to contact members of staff*

## Social media

With an increase in the use of all social media for professional and personal purposes, it is essential to have a policy that provides clear guidance to staff on how to manage risk and behaviour online. One of the key messages is to ensure that learners, the school/college and individuals are protected when publishing any material online.

Professional behaviour expectations for staff are set by the General Teaching Council for Wales (GTCW), but all adults working with children and young people must understand that the nature of their work and responsibilities places them in a responsible position, and their behaviour should reflect that.

All schools/colleges and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Indirectly, schools/colleges and local authorities may be seen to be responsible for the actions of their employees during their employment. If a member of staff is upset, bullies online, discriminates on the grounds of gender, race or disability, or defams a third party, it can make the school/college or local authority accountable to the victim. Reasonable steps must be determined to prevent foreseeable harm. All staff working in any educational establishment are expected to be able to behave professionally and respect learners and their families, colleagues and the learning setting.

To ensure that reasonable steps are in place to reduce the risk of harm, the school provides the following measures:

- ensure that personal information is not published
- provide training that includes acceptable use, social media hazards, checking settings, data protection and reporting on issues
- provide guidance on reporting, including responsibilities, order and sanctions
- risk assessment, including legal risk.

School/college staff should ensure that:

- there is no reference to learners, parents and carers or to school staff on social media
- do not discuss personal issues online relating to members of the school community
- personal opinion is not attributed to the school or to the local authority
- security settings on personal social media profiles are frequently checked to reduce the risk of losing personal information

When the official social media accounts of the school/college are set up, they should be ensured that they have:

- process for senior officer approval
- clear processes for administering and monitoring the accounts – including at least two members of staff
- code of conduct for account users
- systems for reporting and dealing with abuse and misuse
- an understanding of how cases can be dealt with under the school/college disciplinary procedures

**Personal use**

- Personal communication is the communication made on personal social media accounts. In all cases, if a personal account associated with the school/college or affecting the school/college is used, it must be clearly stated that the member of staff does not communicate on behalf of the school/college with an appropriate disclaimer. Details of such personal communication are in the scope of this policy.
- Personal communication that does not refer to or affect the school is outside the scope of this policy.
- If there is a suspicion of excessive use of social media for personal purposes at school, which is believed to interfere with relevant duties, disciplinary action may be taken.
- *The school allows reasonable and appropriate access to private social media sites.*

**Monitoring public social media**

- As part of social media involvement, constant monitoring of the Internet for public comments about the school/college is felt to be good practice.
- The school/college should respond effectively to comments on social media made by others, in accordance with a particular policy or process.

The school/college's use of social media for professional purposes will be regularly checked by a senior leader and the online safety committee to ensure compliance with social media, data protection, communications, digital images and video policies.

The social media policy template at Annex B4 provides more detailed guidance on school/college responsibilities and good practice.

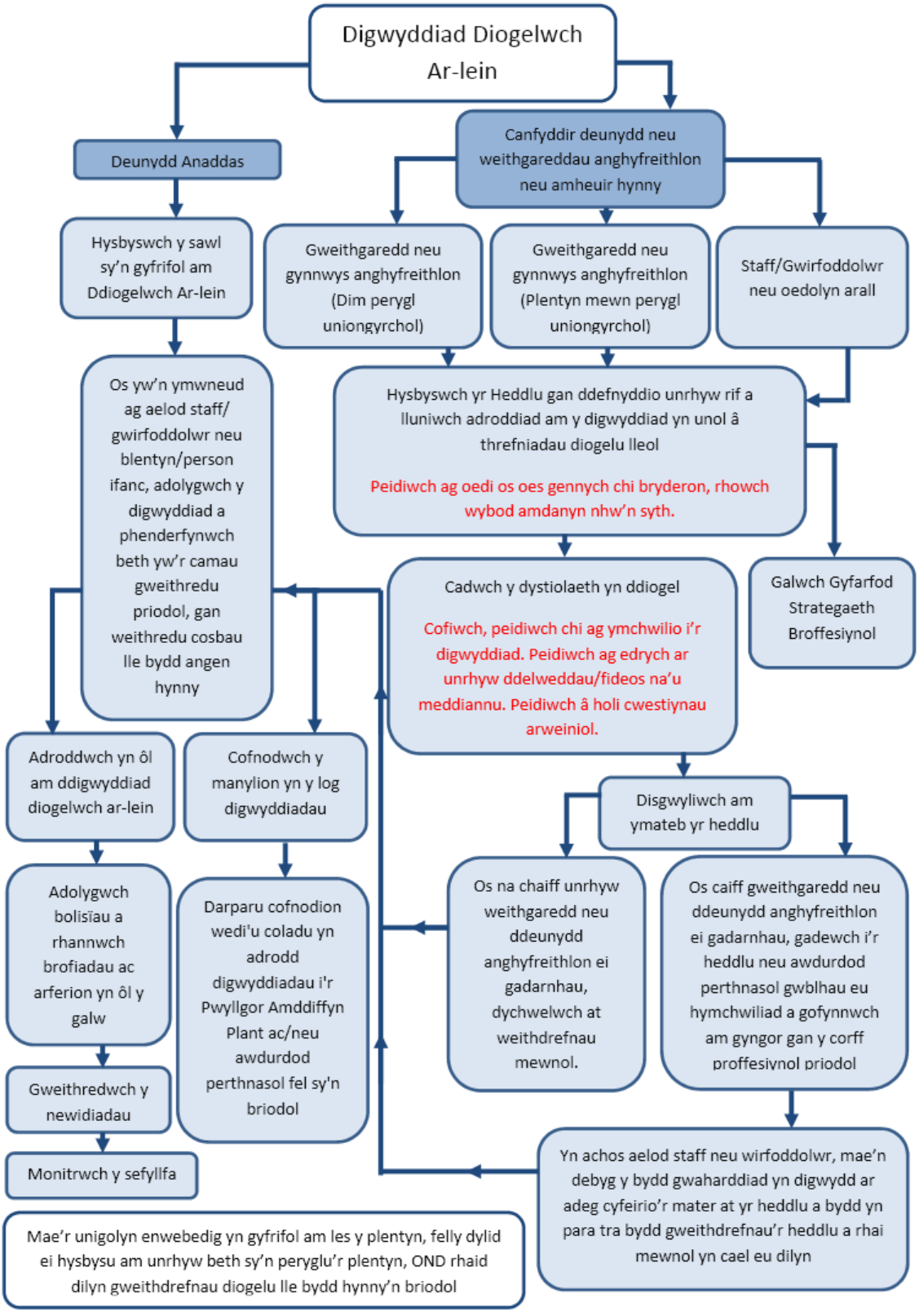
## Inappropriate / inappropriate activities

Some activities on the internet are illegal, for example accessing images of child abuse or sharing racist material. Clearly, this will be excluded from school/college and all other technical systems. Other activities, such as online bullying will be banned and this can lead to criminal prosecution. There are some activities that may generally be legal but are inappropriate in a school/college context because of the age of the users or the nature of the activities.

The school/college believes that the activities in the following section would be inappropriate in the context of the school/college and that users should not participate in them in school or outside school/college when using school/college equipment or systems. The school's policy restricts use as follows:

| User Actions | | Acceptable | Acceptable at certain times | Acceptable to nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not visit, create, post, download, download, transmit data, communicate or pass, material, offers or comments containing or related to: | images of child sexual abuse - the creation, production or distribution of indecent images of children, contrary to the Protection of Children Act 1978 | | | | | X |
| | grooming, encouraging, organising or facilitating sexual acts against children, contrary to the Sexual Offences Act 2003 | | | | | X |
| | possess an extreme pornographic image (which is shockingly indecent, disgusting or otherwise of an obscene nature), contrary to the Criminal Justice and Immigration Act 2008 | | | | | X |
| | criminal racist material in the UK - to incite religious hatred (or hatred on grounds of sexual orientation) - contrary to the Public Order Act 1986 | | | | | X |
| | pornograffi | | | | X | |
| | promote any form of discrimination | | | | X | |
| | threatening behaviour, including promoting physical violence or mental harm | | | | X | |
| | promoting extremism or terrorism | | | | X | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | any other information that may insult colleagues or lack the integrity of the school/college ethos or bring the school/college into disrepute | | | | X | |
| Use of school/college systems to run a private business | | | | | X | |
| Use systems, apps, websites or other mechanisms that avoid filtering or other protection used by the school/college | | | | | X | |
| Copyright infringement | | | | | X | |
| Highlight or publish confidential or owned information (e.g. fiscal/personal information, databases, access codes and computer/network passwords) | | | | | X | |
| Create or spread computer viruses or other harmful files | | | | | X | |
| Unfair use (downloading/downloading large files that prevent others from using the internet) | | | | | X | |
| Play online games (educational) | | x | | | | |
| Play online games (not informative) | | | | | x | |
| Online gambling | | | | | x | |
| Shopping/online trade | | | x | | | |
| File sharing | | | | x | | |
| Using social media – E.g. SCHOOL TWEETS | | | | x | | |
| Use messaging apps – e.g.When connecting on whats app to convey a key message to another member of staff | | | | x | | |
| Broadcasting videos e.g. YouTube – part of school work especially during lockdown | | | | x | | |


Digwyddiad Diogelwch Ar-lein
Deunydd Anaddas
Canfyddir deunydd neu weithgareddau anghyfreithlon neu amheuir hynny
Hysbyswch y sawl sy'n gyfrifol am Ddiogelwch Ar-lein
Gweithgaredd neu gynnwys anghyfreithlon (Dim perygl uniongyrchol)
Gweithgaredd neu gynnwys anghyfreithlon (Plentyn mewn perygl uniongyrchol)
Staff/Gwirfoddolwr neu oedolyn arall
Os yw'n ymwneud ag aelod staff/ gwirfoddolwr neu blentyn/person ifanc, adolygwch y digwyddiad a phenderfynwch beth yw'r camau gweithredu priodol, gan weithredu cosbau lle bydd angen hynny
Hysbyswch yr Heddlu gan ddefnyddio unrhyw rif a lluniwch adroddiad am y digwyddiad yn unol â threfniadau diogelu lleol
Peidiwch ag oedi os oes gennych chi bryderon, rhowch wybod amdanyn nhw'n syth.
Cadwch y dystiolaeth yn ddiogel
Cofiwch, peidiwch chi ag ymchwilio i'r digwyddiad. Peidiwch ag edrych ar unrhyw ddelweddau/fideos na'u meddiannu. Peidiwch â holi cwestiynau arweiniol.
Galwch Gyfarfod Strategaeth Broffesiynol
Adroddwch yn ôl am ddigwyddiad diogelwch ar-lein
Cofnodwch y manylion yn y log digwyddiadau
Disgwyliwch am ymateb yr heddlu
Adolygwch bolisïau a rhannwch brofiadau ac arferion yn ôl y galw
Darparu cofnodion wedi'u coladu yn adrodd digwyddiadau i'r Pwyllgor Amddiffyn Plant ac/neu awdurdod perthnasol fel sy'n briodol
Os na chaiff unrhyw weithgaredd neu ddeunydd anghyfreithlon ei gadarnhau, dychwelwch at weithdrefnau mewnol.
Os caiff gweithgaredd neu ddeunydd anghyfreithlon ei gadarnhau, gadewch i'r heddlu neu awdurdod perthnasol gwblhau eu hymchwiliad a gofynnwch am gyngor gan y corff proffesiynol priodol
Gweithredwch y newidiadau
Monitrwch y sefyllfa
Yn achos aelod staff neu wirfoddolwr, mae'n debyg y bydd gwaharddiad yn digwydd ar adeg cyfeirio'r mater at yr heddlu a bydd yn para tra bydd gweithdrefnau'r heddlu a rhai mewnol yn cael eu dilyn
Mae'r unigolyn enwebedig yn gyfrifol am les y plentyn, felly dylid ei hysbysu am unrhyw beth sy'n peryglu'r plentyn, OND rhaid dilyn gweithdrefnau diogelu lle bydd hynny'n briodol

# Responding to misuse

It is intended that this guidance will be used when staff need to manage events that include the use of online services. It encourages a safe approach to incident management. Incidents may involve illegal or unsuitable activities (see 'User actions' section above).

## Illegal Incidents

If there is any doubt that the website or websites in question contain images of child abuse, or if any otherwise illegal activity is suspected, please refer to the right hand side of the flowchart (below and in the appendices) to respond to online safety incidents and inform the police immediately.

## Other events

It is hoped that all members of the school community use digital technologies responsibly, understand and follow the school's policy. But there may be shortcomings to the policy at times, in abusing them negligently, irresponsibly or (rarely) intentionally.

**In the event of suspicion, all the stages of this procedure should be followed.**

- Get more than one senior member of staff/volunteers involved in the process. The protection of individuals is essential if allegations are made at a later date.
- Carry out the procedure using a designated computer that is not used by learners and can be removed from the site by the police if necessary. Use the same computer during the procedure period.
- It is important to ensure appropriate internet access for relevant staff so that they can carry out the procedure, but that the websites and content visited are closely monitored and recorded (to better protect).
- Record the URL of websites containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and save screenshots of the content on the machine being used for the investigation. These may be printed, signed and attached to the form (except in cases of child sexual abuse images - see below).
- Having fully examined this the group will need to decide whether or not there is substance to this concern. If yes, appropriate action will be required and this may include the following actions:
    - internal response or disciplinary procedures
    - contact the local authority or national/local organisation (as applicable).
    - police involved and/or operating
- **If the content under review contains images of child abuse then monitoring and notification to the police should be stopped immediately. Other examples of cases that should be reported to the police are:**
    - events involving preparation for sex purpose (grooming)
    - send indecent material to a child
    - material for adults who may be in breach of the Indecent Publications Act
    - criminal racist material

- promoting extremism or terrorism
- conduct, activity or otherwise criminal material

- Isolates the computer in question as best as possible. Any change to his condition may damage later police investigations.

It is important that all of the above steps are followed as they will provide an evidence trail to the school/college and possibly to the police, and show that visits to these websites have been made for safeguarding purposes. The group should keep the completed form as evidence and for reference.

### School operations:

It is more likely that the school will need to deal with incidents involving inappropriate rather than illegal misuse. It is important to respond quickly to any incidents in a proportionate manner, and that members of the school/college community are aware that there has been a response to incidents. The intention is to deal with incidents of abuse through normal conduct/disciplinary procedures as follows:

# Learners' actions

| Events | Referring to a teacher / class tutor | Referral to Head of Department / Head of Year / other | Referral to the Headteacher | Referral to the Police | Referral to technical support staff for filtering / safety action etc | Informing parents / carers | Remove network / internet access rights | Notice | Further penalty e.g. detention / exclusion from school/college |
|---|---|---|---|---|---|---|---|---|---|
| Accessing or attempting to access material that may be considered illegal (see list in earlier section on unsuitable / inappropriate activities). | | X | X | X | | | | | |
| Use of non-educational websites during unauthorised lessons. | X | X | | | | | | | |
| Unauthorised use of mobile phones/digital camera/other mobile devices. | | X | X | | | X | | X | X |
| Unauthorized use of social media/personal email/messaging apps. | | X | X | | | X | | X | X |
| Download or download unauthorized files. | | X | X | | | X | | X | X |
| Allow others to access the school/college network when sharing a username and password. | | | X | X | X | | | | |
| Seek, or access the school/college network using another learner's account. | | | X | X | X | | | | |
| Seek, or access the school/college network using a staff member's account. | | | X | X | | X | X | X | X |
| Corrupting or destroying other users' data. | | X | X | | | X | X | X | X |
| Send an abusive email, text or message, which is painful or has the nature of bullying. | | X | X | X | | X | X | X | X |
| Persistent breaches of the above rules, following advance warnings or sanctions. | | | | | | X | | | X |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Activities that can bring the school/college into disrepute or spoil the ethos of the whole school/college. | | X | X | | | X | X | X | X |
| Use proxy websites or other means to overturn the school/college filtering system. | | | | | X | | | | |
| Gain access to offensive or pornographic material by accident and not report the incident. | | X | X | | | X | X | X | |
| Obtaining, or attempting to access offensive or pornographic material. | | X | X | X | X | X | X | X | X |
| Obtaining or transmitting material that in breach of another person's copyright or in breach of the Data Protection Act. | | X | X | | x | X | X | X | |

## Gweithrediadau Staff

| **Events:** | Referring to the line manager | Referral to the Headteacher | Referral to local authority / Human Resources | Referral to the police | Referral to Technical Support Staff for filtering action | Notice | Ban | Disciplinary Action |
|---|---|---|---|---|---|---|---|---|
| **Accessing or attempting to access material that may be considered purposefully illegal (see list in earlier section on unsuitable/inappropriate activities)** | | x | x | x | | X | X | X |
| Unsuitable personal use of the internet/social media/personal e-mail | X | X | | | | | | |
| Download or download unauthorized files. | X | X | | | | X | | |
| Allow others to access the school/college network when sharing a username and password or trying, or accessing the school/college network using another person's account. | X | X | | | | | | |
| Irresponsible use of personal data e.g. unsafe retention or transfer of data | X | X | X | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Act intentionally to contravene data protection or breach network security rules. | | X | X | X | | | | |
| Corrupting or destroying other users' data or causing deliberate damage to hardware or software | | X | X | | X | X | X | X |
| Send an email, text or message that is offensive, painful or contains the nature of bullying | X | X | X | | | | | |
| Use personal e-mail/social networking/send messages to communicate digitally with learners<br>- STAFF NEED TO USE HWB EMAIL ONLY FOR COMMUNICATION | X | X | X | | | | | |
| Activities that may compromise the professional status of a member of staff | x | x | x | x | x | x | x | x |
| Activities that could bring the school/college into disrepute or spoil the ethos of the whole school/college. | | | | | | | | |
| Use proxy websites or other means to overturn the school/college filtering system. | | x | x | | | | | |
| Gain access to offensive or pornographic material by accident and not report the incident. | x | x | x | | | x | | |
| Obtaining, or purposefully attempting to access offensive or pornographic material. | x | x | x | x | x | x | x | x |
| Infringement of copyright or licensing rules. | x | x | x | | | x | | |
| Persistent breaches of the above rules, following previous warnings or sanctions. | | | | | | | | X |

Head Teacher's signature:

Date: 15.10.26

Chair of GB signature:

| | |
|---|---|
| Version: | 04 |
| Review Date: | Autumn 2027 |