BRYN-Y-DERYN

CARNEGIE CENTRE

Cyfleoedd ar gyfer newid a llwyddiant

Opportunities for change and success

Online Safety Policy
2021-2022

Acceptable use policy

All members of staff and learners must to sign an acceptable ICT use agreement before using any school ICT resource. A record of all staff and learners who have been granted Internet access is kept by the ICT technician. Internet access is also discussed during the admission interview with the Head of Centre. A record is then kept on Sims.

All members of staff are expected to adopt a common sense approach to the use of ICT equipment and software that takes account of social, professional and legal responsibilities and the age-related vulnerability of the young people in our care.

Bryn y Deryn acknowledges the educational and social benefits of ICT facilities.
All members of the school community (staff and learners) are expected to adopt a common sense approach to the use of ICT equipment and software that takes account of social, professional and legal responsibilities, and the age-related vulnerability of the young people in our care.

Inconsiderate or inappropriate use of systems may result in:

- Disciplinary action for staff including the possibility of dismissal
- Disciplinary action for learners including the possibility of exclusion
- The possibility of legal action for either staff or learners

In the case of both learners and staff:

- The ICT facilities should normally only be used in connection with work associated with the school and not for personal or private communication. However, limited and appropriate personal use is acceptable, for example during the lunch breaks or before or after the school day.
- Computer facilities must not be used to offend or harass, either within or outside the School and Individuals should never disrupt, interfere with or prevent anyone else using the facilities legitimately.
- Certain acts are considered particularly inappropriate and will lead to action.
  - The use of computer facilities to offend or harass;
  - The sending or relaying of sexist / racist / defamatory / indecent / obscene / pornographic / violent / offensive e-mails, data or images;
  - The accessing of sexist/racist/indecent/defamatory/obscene/pornographic/ violent/offensive material;
  - The downloading, storage and distribution of such material;
  - The creation of a website or screen saver of such material;
  - The use of the School's ICT facilities for commercial gain or for work on behalf of others unless prior agreement has been made with the designated authority;
  - The deliberate misuse of the network or networked resources, such as introducing "viruses", violating the privacy of others;
  - The theft, abuse or wilful damage of computer equipment;
  - the misappropriation of software or other copyright material belonging to another person or institution
  - The sale, import and distribution of copies of software without the permission of the copyright owner.

The above list is not intended to be exhaustive, but an indication of the types of act that would be dealt with under the school's Disciplinary Code and Procedures.

Entering into contracts online

Many web-based services providing teaching materials etc. require staff to create user accounts. It is the duty of the member of staff creating the account to read the terms and conditions fully before creating the account, to ensure that they are not entering into a contractual relationship for the supply of goods and services that may incur charges. In some case such terms and conditions are not made clear on the website. Goods and services can only be purchased by staff following the Finance procedures.

Social Media and Messaging

Internet based systems that enable messaging

Systems that provide the facility to message learners are useful in supporting their learning but can also pose risks. These systems would include social media (such as Facebook), but also include games and any website where messages can be posted, or transmitted live (e.g. MSN or Twitter).

Staff must not communicate with learners or recent ex-students using personal accounts. If these systems are to be used the following limitations apply:

1. Accounts must be named after departments, activities or projects, not named individuals
2. Accounts and profiles should make it clear that their use is part of school life
3. Usernames and passwords are to be shared with the line manager of the member of staff responsible for using the service
4. The line manager is given a clear explanation of the purpose of the use and the type of content that will be transmitted
5. Where a homepage, profile or site is created consideration must be given as to whether postings by other users (outside of the editorial control of the school) can be prevented or removed should they be defamatory

As a general principle official communication from the school should be via systems owned and controlled by the school, ensuring that all the information presented as being associated with the school is appropriate. Systems outside the control of the school must meet this requirement before official school communication is transmitted.

Personal staff social media

Staff are reminded that it is in the nature of social media systems that content can be viewed by a wide, and often unpredictable audience. Once content (images, video, audio or text) has been posted control over its audience is effectively lost. Staff are therefore advised to review both the content of their current social media profiles, and their security settings to minimise any potential reputational risk to themselves or the school.

Misuse of Social Media that affects the school community

All incidents of inappropriate use of social media are taken seriously and we encourage all members of the school community to report any incidents of inappropriate use of social media and interactive technology.

Inappropriate use of social media includes, but not restricted too:

- harassment and intimidation of others,
- sending hateful messages,
- posting inappropriate and unwanted pictures online,
- creating content which has the potential to hurt, embarrass and humiliate others,
- Sexting (creating and sending, or granting access to sexual images of yourself to another)
- Grooming,
- Online exploitation including sexual abuse

We respond to inappropriate use and bullying online in accordance with the procedures and guidance outlined in our anti-bullying and behaviour policy. Support is provided to all parties involved in incidents of bullying online and parents will be notified following a report of bullying online. Where appropriate we will contact external agencies to obtain further advice, information and provide additional support to individuals if necessary. Restorative approaches will be implemented to resolve any issues of inappropriate use of social media. We understand that in some circumstances there will be a requirement to involve the police. We will liaise with our Police School Liaison Officer for advice on the appropriate route and action to take in these circumstances. The school reserves the right to search the content of any mobile or handheld devices on the school premises. School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour policy or bullying procedures

All staff are required and students are encouraged to report any message or content they feel is inappropriate via MyConcerns. IT staff will liaise with the Learners Protection Officer and pastoral staff should there be evidence of risk or harm.

Extremist material or behaviour using computers (PREVENT)

The young people we are responsible for are particularly vulnerable to extremist material, and attempts at contact from extremists, due to the extent of their use of online social media. Any learners or young person experiencing this situation is at risk of harm. Many young people may have Internet access on smartphones that is not filtered or restricted for their protection.

All staff supervising learners need to be aware of these risks, and have a duty to act should they become aware of such material or activities, and must:

- Make a record of what was seen or heard, including a note of the system, website or service being used to transmit the messages or media, and the device or PC being used
- Make a Learners Protection referral (see Learners Protection Policy)
- Copy information sent to thesafeguarding team and log in MyConcerns

The following file gives more information about the ways radical groups use social media: How_social_media_is_used_to_encourage_travel_to_Syria_and_Iraq.pdf

Inappropriate sexual activity or grooming

All staff supervising learners should be aware that ICT devices of all kinds can be used by abusive individuals to enter into exploitative relationships with learners. These learners are then exploited for sexual gratification, which often involves the transmission of indecent images of the learners created under duress. This behaviour can also be the result of dysfunctional relationships between learners, with bullying based on the misuse of images and material exchanged during the relationship.

You may come across evidence of indecent content on devices, and you should make a written or digital record of what you have seen, the device and systems (social media) used. **You must then record all information onto MyConcerns**

A learner who is in difficulty in this way may behave in an uncharacteristic way, especially about their phone or device. They may check their device more frequently, or may withdraw from others just to look at their device. They may be visibly upset or defensive about using their phone or showing it to others.

More information about these issues is available from the Learners Exploitation and Online Protection Command website (CEOP).
https://www.thinkuknow.co.uk/Teachers/

Monitoring of Systems

The School gives notice of its ability to monitor and intercept information for the purposes of.

- Establishing the existence of facts (e.g. to obtain evidence of business transactions)
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using its systems (e.g. for staff training or quality control);
- Preventing or detecting crime
- Investigating or detecting unauthorized use of the system (e.g. to check that users are not downloading pornography)
- Ensuring the effective operation of this system (e.g. to protect against "viruses", "worms", denial of service attacks, unauthorized access)

Monitoring is allowed under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, made under the Regulation of Investigatory Powers Act 2000, but is also subject to the provisions of the Human Rights Act 1998 and the Data Protection Act 1998. Authorised IT Systems Administrators require access to data held on ICT equipment or transferred over the network to ensure that networks, systems and services are operating correctly. Any information obtained in the course of such duties will be treated as confidential unless it is thought to indicate an operational problem.

Any information that is thought to indicate misconduct or breach of school policies will be brought to the attention of the Head of Centre. If deemed appropriate, further monitoring of IT and network equipment may be carried out to ensure compliance with school policies which apply to these systems. Monitoring of an individual's ICT facilities will only be carried out when there is reason to suspect misuse and will only be carried out at the request or authorisation of the Head of Centre.

Software Issues

a) Software Legal Requirements.

Staff and learners must adhere at all times to statutory law, including.

- The Theft Act 1968.
- The Copyright, Patents and Design Act 1988.
- The Computer Misuse Act 1990.

All software within the School must be obtained legally and used in accordance with the licensing arrangement.

School licensed software must not be copied without the express prior written consent of the ICT Department, and then only where the license permits.
Making copies of software without the permission of the copyright owner is an infringement of copyright law.

b) Software Procurement and Registration.

All software must either be purchased or approved via the ICT Department. Departments wishing to purchase software from their departmental budgets should discuss their requirements with the ICT department prior to purchase. *(See IT guidance & procedures in the white section of the handbook for further information)*

Unauthorised or non-standard software may not be installed unless prior consent from the ICT Department is obtained. Consent is given for staff to install freeware, open source software, demonstration software and other licensed software required for teaching.

The ICT Department maintains a software record log.

c) Home Use

Some software licenses allow the software to be used at home by staff. Often there will be restrictions on the use of the software for example, for use for work related purposes only. In all such licenses the user must stop using the software when they are no longer a member of the School.

d) Viruses

Every effort must be made to ensure that computer viruses are not introduced into School. All School PCs run anti-virus software, which is updated regularly. On PCs this is an automatic process.

The creation / introduction of viruses to a computer is regarded as an unauthorised modification of computer material by the Computer Misuse Act. Such an action is an offence, which may be punished with up to 5 years imprisonment.

Information & Security – Legal Requirements

a) Information and Security Legal Requirements

Staff and learners must at all times adhere to statutory law, including.

- The Data Protection Act 1998.
- The Computer Misuse Act 1990.
- General Data Protection Regulations 2018 (GDPR)

b) Passwords

User passwords must not be shared. It is therefore important that staff save lesson materials, which might be used for cover lessons in the event of absence, to the staff shared area and / or Moodle instead of their own space so that it can be accessed by others if necessary.

Individuals must take every precaution to ensure the privacy of their password and individuals will be held accountable for its misuse.
Learner passwords are set to a default, which must be changed at the first available opportunity. This is the responsibility of the learner.
Users are required to log off or lock their workstation if they leave their systems unattended.

The Network Manager will ensure that the network policy settings force staff to change their passwords once every term.

Unauthorised Access to Computers.

Unauthorised access to computer held information is illegal. Unauthorised access to computer material is forbidden by the Computer Misuse Act 1990.

a) Email

Email is a primary means of communication within the school. Both staff and learners should therefore check their mailboxes on a daily basis. In general, email should only be used in connection with activities related to the school, but reasonable limited use is acceptable.

Authorisation from the Head of Centre is required to access the Email account of another member of staff who is absent. Only the person’s line manager will be permitted such access and the person must be informed on their return that such access has been granted.

b) Internet

The school acknowledges the educational and social benefits of the use of the Internet. The Internet should not be used for personal or private activities unrelated to school life, but reasonable limited use is acceptable.

c) File storage

Bryn y Deryn provide personal file storage space for staff and learners, and shared storage space for staff. This information is backed up daily to allow recovery of information in the events of a system failure.
Authorisation from the Head of Cenre is required to access the personal storage area of another member of staff who is absent and the person must be informed on their return that such access has been granted.

d) Network Use
Staff, learners and visitors may not connect equipment into the school's network without the agreement of the ICT Technician. Any data which due to its nature, content or size, is likely to significantly affect the operation of the school network may only be transmitted subject to agreement with the ICT Technician.

Equipment

a) Procurement of ICT Equipment
All IT equipment must be purchased through the ICT Technician.

b) Inventory/Security of Equipment.
All equipment is recorded on School inventories. Any School equipment that is loaned to a member of staff is their responsibility and they must sign a loan form which must be authorised by the ICT Technician or Head of Centre. The individual or their department will bear the cost of replacement or repair of the equipment should it be damaged, lost or stolen in any way.

c) Equipment Change of Use/Location.
Computer equipment may only be used for purposes other than its 'intended' purpose following written approval from the ICT co-ordinator or Head of Centre.

d) Provision of ICT Equipment
The school aims to provide replacement PCs for staff and student every five years. This is provided centrally. The school aims to provide replacement laptop/notebooks every three years.

e) Disposal of IT Equipment
The ICT Technician is responsible for the disposal of all IT equipment within the school. All unwanted IT equipment must be returned to the ICT Department. All equipment that is scrapped will be disposed of in accordance with Waste Electronic and electrical equipment (WEEE) legislation.

Equipment that is no longer required by the School will be offered for sale, in the first instance to school staff or learners. Any equipment that is sold or donated will be wiped of all data in accordance with The Data Protection Act 1998 and GDPR. If equipment cannot be sold by the school then it can either be donated to charities / schools (if the school is satisfied that reuse of the equipment is viable), or scrapped in an environmentally sound way according to WEEE legislation.

f) Health & Safety
All equipment must be used in compliance with Health & Safety Regulations. Copies of Health & Safety Regulations are available from the School Health & Safety Officer.

Links to other policies

This policy links with a number of other policies, practices and action plans including:

- Anti-bullying policy
- Behaviour and discipline policy
- Learners protection policy

- Curriculum policies, such as: Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE)
- GDPR

Roles and responsibilities

The school e-safety co-ordinator is Mr T Leahy
The Digital Competency Co-ordinator is Miss Cole
The designated member of the management committee responsible for e-safety is A Cook
The safeguarding team consist of Miss Simpson, Mr Bevan, Mrs Howells and Mr Francis.

Staff Training

All staff have completed an ICT skills audit and there are opportunities for staff development and training, highlighted on the school calendar.

Parental involvement

All parents will be made aware of the school online safety policy through the School Website, in the school prospectus and in newsletters.

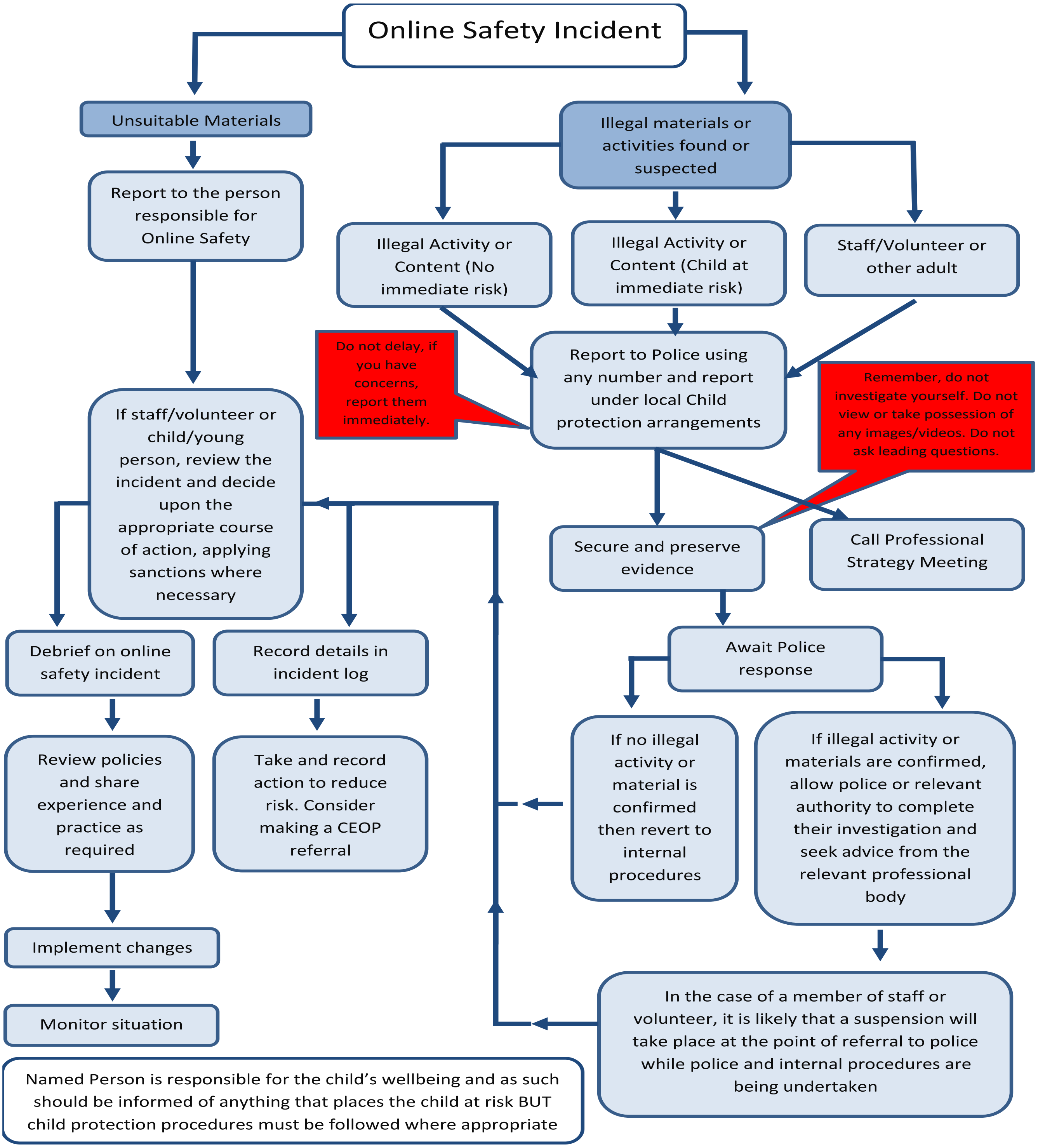
How images and film are managed

All parents are asked to sign an agreement during the pupil admission meeting. However, it is the responsibility of all staff to ensure that a parent has given permission, for their learners's image to be used, before the image is taken. The names of those parents who have given their permission for their learners's image to be used is stored on SIMS. All images are stored securely on the shared drive.

How e-safety is covered in the curriculum

The are many opportunities for e-safety to be covered across all subject areas including pastoral time.

How incidents are reported



Online Safety Incident

Unsuitable Materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review policies and share experience and practice as required

Take and record action to reduce risk. Consider making a CEOP referral

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Illegal Activity or Content (No immediate risk)

Illegal Activity or Content (Child at immediate risk)

Staff/Volunteer or other adult

Do not delay, if you have concerns, report them immediately.

Report to Police using any number and report under local Child protection arrangements

Remember, do not investigate yourself. Do not view or take possession of any images/videos. Do not ask leading questions.

Secure and preserve evidence

Call Professional Strategy Meeting

Await Police response

If no illegal activity or material is confirmed then revert to internal procedures

If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police while police and internal procedures are being undertaken

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk BUT child protection procedures must be followed where appropriate

*Signed:*______________________________

F. Simpson

Head of Centre

*Signed:*______________________________

J. Heerey

Chair of Management Committee