BRYN-Y-DERYN

CARNEGIE CENTRE

Cyfleoedd ar gyfer newid a llwyddiant

Opportunities for change and success

Online Safety Policy

2023 – 2024

For the purpose of this policy Bryn y Deryn (BYD) means BYD & Carnegie Centre (CC)

Acceptable use policy

All members of staff and learners must to sign an acceptable ICT use agreement (see appendix A) 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.

There must be a strong pedagogical or business reason for creating official school sites to communicate with learners or others. Staff must not create sites for trivial reasons which could expose the school to unwelcome publicity or cause reputational damage. Schools must also ensure that Parent Teacher Associations that may set up sites to promote school events to advertise within the school community are aware of this policy.

Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

Personal staff social media

Staff members must not identify themselves as employees of Bryn y Deryn & Carnegie. This is to prevent information on these sites from being linked with the school and Cardiff Council and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.

Staff members are strongly advised not to have contact through any personal social medium with any learner, whether from Bryn y Deryn & Carnegie or any other school, unless the learners are family members.

Bryn y Deryn & Carnegie does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.

Staff members must not have any contact with learners' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.

If staff members wish to communicate with learners through social media sites or to enable learners to keep in touch with one another, they can only do so with the approval of the school and through official school sites created according to the requirements specified in section 7.

Staff members must decline 'friend requests' from learners they receive in their personal social media accounts. Instead, if they receive such requests from learners who are not family members, they must discuss these in general terms in class and signpost learners to become 'friends' of the official school site.

On leaving Bryn y Deryn & Carnegie's service, it is advisable that staff members do not contact Bryn y Deryn & Carnegie's learners by means of personal social media sites. Similarly, staff members must not contact learners from their former schools by means of personal social media.

Information staff members have access to as part of their employment, including personal information about learners and their family members, colleagues, Cardiff Council staff and other parties and school or Cardiff Council corporate information must not be discussed on their personal webspace.

Photographs, videos or any other types of image of learners and their families or images depicting staff members wearing school or Cardiff Council uniforms or clothing with school or Cardiff Council logos or images identifying sensitive school or

Cardiff Council premises (eg care homes, secure units) must not be published on personal webspace. This includes images of learners/staff on any school-based activity whether in school uniform or not.

School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

Bryn y Deryn & Carnegie or Cardiff Council corporate, service or team logos or brands must not be used or published on personal webspace.

Bryn y Deryn & Carnegie only permits limited personal use of social media while at work in line with the Cardiff Council Social Media and Internet Acceptable Use policies. Staff members are expected to devote their contracted hours of work to their professional duties and, in practice, personal use of the internet should not be on the school's time.

Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites as social networking sites can blur the line between work and personal lives.

Staff members are strongly advised to review their privacy settings and understand who will see your personal information and content you publish. Staff members should keep their passwords confidential, change them often and be careful about what is posted online, it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

Staff members should be aware that information posted publicly on social media is instantly available across the world and that online conversations can never be fully private.

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.

Breaches of this policy

Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with Bryn y Deryn & Carnegie Disciplinary Policy and Procedure.

A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of Bryn y Deryn & Carnegie or Cardiff Council or any illegal acts or acts that render Bryn y Deryn & Carnegie or Cardiff Council liable to third parties may result in disciplinary action or dismissal.

Cardiff Council services must inform the relevant school or a Cardiff Council officer immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the school and Cardiff Council. Any action against breaches should be according to contractors' internal disciplinary procedures.

There are a number of categories into which social networking/social media problems for schools can fall:

- interaction between learners
- interaction between teaching staff
- interaction between learners and teaching staff
- interaction between teaching staff and parents
- unpleasant/abusive postings about teaching staff
- postings that are critical of leadership/management of school

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:
https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

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.

Unauthorised or non-standard software may not be installed unless prior consent from the ICT Department is obtained. ICT will submit a ticket to ICT support (Cardiff Council) for the software to be installed by a technician. This can take up to 3 weeks.

c) Home Use

Some software licenses allow the software to be used at home by staff (Adobe Creative Cloud). 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. HWB Accounts will be either migrated to another School the staff are working at or deleted once he staff has left 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 (Cardiff Council) 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 or data 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 Centre 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.

Files must not be stored on a personal computer when working from home. If working at home staff should use Laptops that where released from Cardiff Council. Bryn y Deryn & Carnegie have access to staff one drives via office 365 or encrypted USB sticks is a staff member is required to transport data from school to home.

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 and Cardiff ICT support.

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 four 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 Collect by Cardiff Council ICT support. This will then be assessed for redeployment or disposed in accordance with Waste Electronic and Electrical Equipment (WEEE).

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
Please see the roles and responsibilities form

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

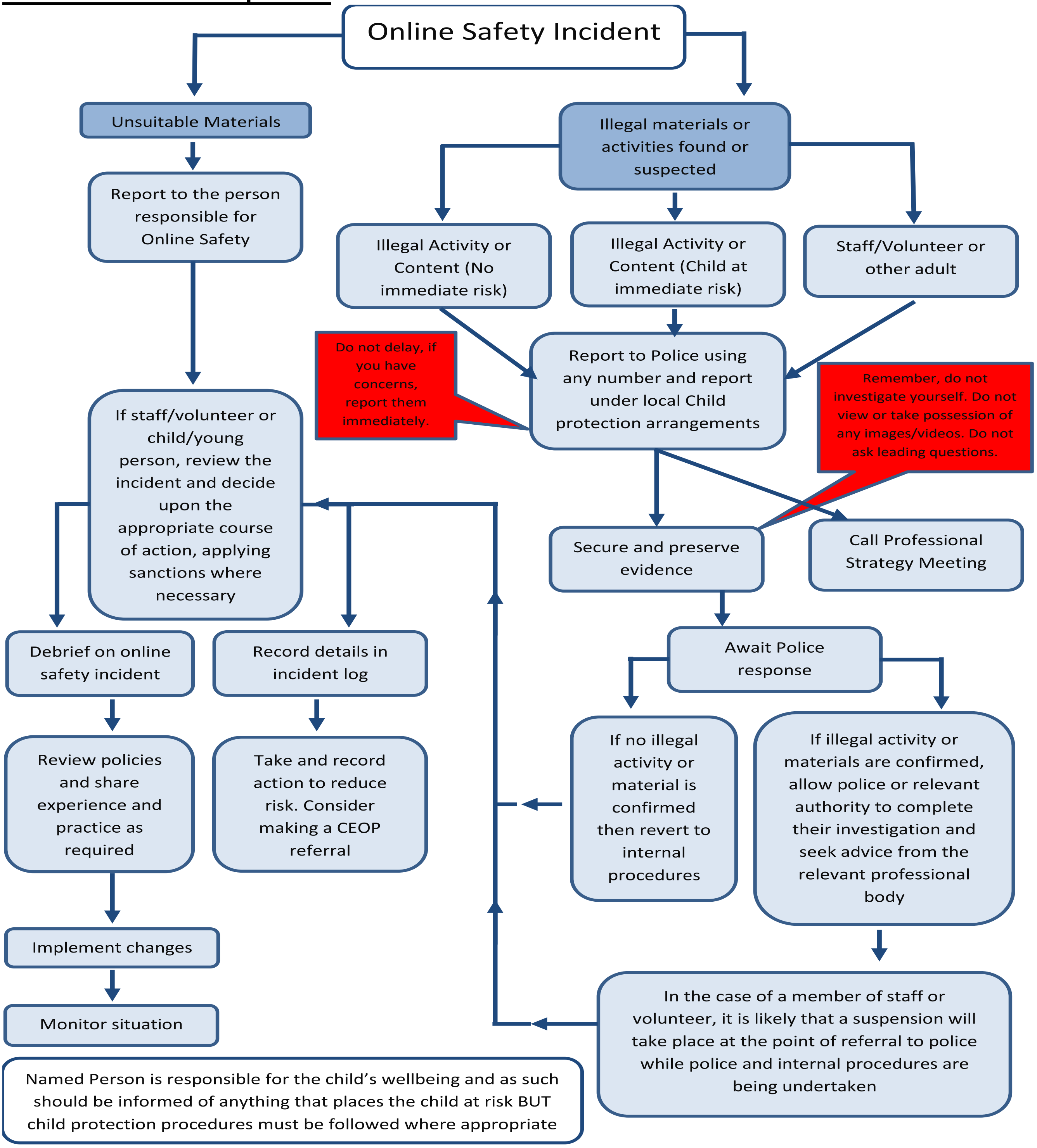
Parental involvement
All parents will be made aware of the school online safety policy through the School Website, in the school prospectus and in newsletters.

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 learner's image to be used, before the image is taken. The names of those parents who have given their permission for their learner'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: BSimpson

F. Simpson

Head of Centre

c y

Signed:

J. Heerey

Chair of Management Committee

Appendix:

Acceptable Use of ICT Agreement for Staff and Volunteers

For the purpose of this policy where you read Bryn y Deryn (ByD) it means Bryn y Deryn & The Carnegie Centre

Acceptable Use of ICT Agreement for Staff and Volunteers

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure that:

- staff and volunteers will act responsibly to stay safer while online, being a good role model for younger users
- effective systems are in place for the online safety of all users and the security of devices, systems, images, personal devices and data
- staff and volunteers are aware of and can protect themselves from potential risk in their use of online technologies

The term "professional" is used to describe the role of any member of staff, volunteer or responsible adult.

For my professional and personal safety, I understand that:

- I will ensure that my on-line activity does not compromise my professional responsibilities, nor bring the school into disrepute
- my use of technology will be monitored
- when communicating professionally I will use technology provided by the school (eg email and school media account
- these rules also apply when using the school's technology either at home or away from the school site
- personal use of school technology is only acceptable with permission
- I will not contact learners via my own personal email
- I will only communicate with learners via my work email about work/professional issues
- When not using my computer, I lock the computer screen
- I will report any possible Data breach to the **Data manager** (T. Leahy) and **Head of Centre**
  (F. Simpson) within 24 hours
- any data being taken home is to be stored on an encrypted USB stick/school device

For the safety of others:

- I will not access, copy, remove or otherwise alter any other user's files, without authorisation
- I will communicate with others in a professional manner
- I will share other's personal data only with their permission

- I understand that any images I publish will be with the owner’s permission and follow the school’s code of practice
- I will only use school equipment to record any digital and video images
- I will check school systems for to confirm that the school has permission to upload digital images or videos to social media

For the safety of the school, I understand that:

- I will not try to access anything illegal, harmful or inappropriate
- it is my responsibility to immediately report any illegal, harmful or inappropriate incident
- I will not share my online personal information (eg social networking profiles) with the children and young people in my care
- I will not deliberately bypass any systems designed to keep school safe
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Personal Data Policy (or other relevant policy). Where personal data leaves the school site, it must be encrypted
- I understand that data protection policy requires that any personal data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by a school policy to disclose such information to an appropriate authority
- personal passwords and those of other users should always be confidential
- I will not download anything that I do not have the right to use
- I will only use my personal device if I have permission and use it within the agreed rules
- I will inform the appropriate person (T.Leahy) if I find any damage or faults with technology
- I will not attempt to install programmes of any type on the devices belonging to the school, without permission
- when not using my computer, I will lock the computer screen
- I will report any possible data breach to the **data manager** (T.Leahy) and **Head of Centre** (F.Simpson) within 24 hours
- any data being taken home is to be stored on an encrypted USB stick/school device or uploaded to the school SharePoint
- I will undertake Bi yearly Cyber safety training
- I will not upload any content to social media sites that:
    - is confidential to the school/trust or its staff
    - amounts to bullying
    - amounts to unlawful discrimination, harassment or victimisation
    - brings the school/trust into disrepute
    - contains lewd, sexually explicit, threatening or similarly inappropriate or offensive comments, images or video clips
    - undermines the reputation of the school and/or individuals
    - is defamatory or knowingly false
    - breaches copyright
    - is in any other way unlawful

Council equipment use outside of school building:
Introduction

- any laptop, computer, iPad, tablet, or mobile device or other (with internet/email facilities) (hereafter referred to as a Computer) issued to you by Cardiff Council or Bryn y Deryn will remain at all times the property of the Company
- it must be clearly understood that the issue of computers to employees is for the purpose of improving the Company's communication systems and is not intended for personal use

Management Responsibilities:

- all computers issued must be authorised by Cardiff Council
- a register of all computers will be maintained and updated as and when required

Security:

- employees issued with a computer must always ensure the security of the computer, this means in work and out of work
- carry and store the computer in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage
- ensure that the computer has been updated to latest settings when turned on each time
- always virus-scan any files downloaded to your computer from any source (CD/DVD, USB hard disks and memory sticks, network files, e-mail attachments or files from the Internet). Virus scans normally happen automatically but the Internal IT Manager can tell you how to initiate manual scans if you wish to be certain
- e-mail attachments are now the number one source of computer viruses. Avoid opening any e-mail attachment unless you were expecting to receive it from that person
- employees are responsible, when away from their work setting to ensure that their issued computer is protected against loss or theft. Bryn y Deryn instructs all employees to adhere to the following:
    - computers must not be left in unattended vehicles
    - keep food and drink away from the computer
    - when travelling by car, computers must be stored securely and out of sight
    - when travelling, computers should not be left unattended in public places
    - it is the responsibility of all staff members to ensure that all laptops are password protected and not to disclose this to anyone
    - only the employee should use the device released to them

Usage:

- computers are for school related use only and not for personal use
- misuse of the Internet and E-mail is regarded as a serious breach of this policy as well as our Data Protection and Acceptable Use policies.
-

In particular, if you view, access, download or distribute pornographic and / or other offensive material from the Internet or send, view, or distribute damaging or offensive e-mails

- unauthorised or unlicensed software must not be loaded on computers
- ensure the computer is not used by unauthorised persons

Working Outside of School or Home:
Follow the following security measures when working outside of home or school to ensure compliance with GDPR.

All mobile devices (including, but not limited to, laptops, tablets and mobile telephones) provided by Cardiff Council or Bryn y Deryn should always be transported securely and handled with care. Users should make all reasonable efforts to avoid such mobile devices from being left unattended at any location other than their homes or school premises.

If any such mobile device is to be left in a vehicle it must be stored out of sight (i.e., locked in the boot or glove compartment depending on size). Where possible the transport of data in paper form containing personal information should be limited/avoided. The use of an encrypted USB is acceptable if there are no other alternatives. Ideally documents should be scanned and used on-line with the exception of where they require signatures. Personal data should not be left in cars. It should be stored securely and returned to School at the earliest opportunity.

If you need to logon to your laptop when out of home or school, please be very cautious when you first access a new network. You may see a terms of use banner, or you may be asked to enter identifying information like an e-mail address. Read the text and be sure to understand how that information might be used. In locations with many Wi-Fi networks available, make sure you're connecting to the right one. Don't fall victim to a rogue hotspot, and don't use an unsecured.

Health and Safety:
Laptops normally have smaller keyboards, displays and pointing devices that are less comfortable to use than desktop systems, increasing the chance of repetitive strain injury, balancing the laptop on your knees does not help the situation. Limit the amount of time you spend using your laptop. Whenever possible, place the laptop on a conventional desk or table and sit comfortably in an appropriate chair to use it. If you tend to use the laptop most of the time, you are advised to use a with a full-sized keyboard, a normal mouse and a display permanently mounted at the correct height. Please liaise with ICT manager Thomas Leahy if you need guidance on create a suitable workspace at home. Stop using the portable if you experience symptoms such as wrist pain, eye strain or headaches that you think may be caused by the way you are using the portable device.