Maes yr Haul Primary School

Ysgol Gynradd Maes yr Haul

Online Safety Policy

ADOPTED: Spring Term 2018 **REVIEW:** Spring Term 2021

Policy Review and Monitoring
This policy is due to be reviewed at the time stated, unless circumstances determine that this policy needs to be reviewed at an earlier time.

Signed: **Chair of Governors** **Headteacher**

Date:

Maes Yr Haul Primary School
Ysgol Gynradd Maes Yr Haul

Enriching Life Through Lifelong Learning
Cyfoethogi Bywyd Trwy Addysg Gydoloes

Online Safety Policy

ADOPTED: Spring Term 2018 **REVIEW:** Spring Term 2021

CONTENTS **PAGE**

Introduction

This policy is based upon the SWGfL 360 degree safe Cymru template and adapted to suit the needs of Maes yr Haul Primary School.

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. This online safety policy has been developed in consultation with the whole school community through a range of formal and informal meetings.

Aims

The purpose of this online safety policy is to:

- safeguard and protect all members of Maes yr Haul Primary School community online.
- identify approaches to educate and raise awareness of online safety throughout the community.
- enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- identify clear procedures to use when responding to online safety concerns.

Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the G*overning Body/governor's sub-committee* receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body should take on the role of online safety governor to include:

- regular meetings with the online safety co-ordinator/officer
- regular monitoring of online safety incident logs
- regular monitoring of filtering change control logs (where possible)
- reporting to relevant governors/sub-committee/meeting

Headteacher and Deputy Headteacher:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- As designated safeguarding leads, (at least) the Headteacher and Deputy Headteacher are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- The Headteacher is responsible for ensuring that staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Online safety co-ordinator:

- leads the online safety group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides (or identifies sources of) training and advice for staff
- liaises with BCBC technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- meets regularly with online safety governor to discuss current issues, review incident logs and raise any concerns with the local authority technical staff.
- attends relevant meeting/sub-committee of governors

BCBC Network manager / technical staff:

The network manager / technical staff are responsible for ensuring:

- that the *school* technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets (as a minimum) the required online safety technical requirements as identified by the local authority or other relevant body and also the online safety policy/guidance that may apply.

- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network/internet/learning platform/Hwb/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher for investigation or action.
- that monitoring software/systems are implemented and updated as agreed in school/LA policies and SLA agreements.
- that the BCBC Internet Security Policy, is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.

Teaching and support staff:

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the staff acceptable use agreement (AUA)
- they report any suspected misuse or problem to the Headteacher for investigation/action
- all digital communications with learners/parents and carers should be on a professional level and only carried out using agreed official school channels
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Learners understand and follow the online safety and acceptable use agreements
- learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc., in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that procedures are followed if dealing with any unsuitable material that is found in internet searches

Designated safeguarding officer (DSO):

The designated safeguarding officer should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Online safety group:

The online safety group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the online safety policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the online safety group will assist the online safety co-ordinator with:

- the production, review and monitoring of the school online safety policy/documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs where possible
- consulting stakeholders – including parents/carers and the learners about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe Cymru self review tool

An online safety group terms of reference template can be found in the appendices

Learners:

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.

Parents and carers:

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website, Hwb, learning platform and information about national/local online safety campaigns/literature.* Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

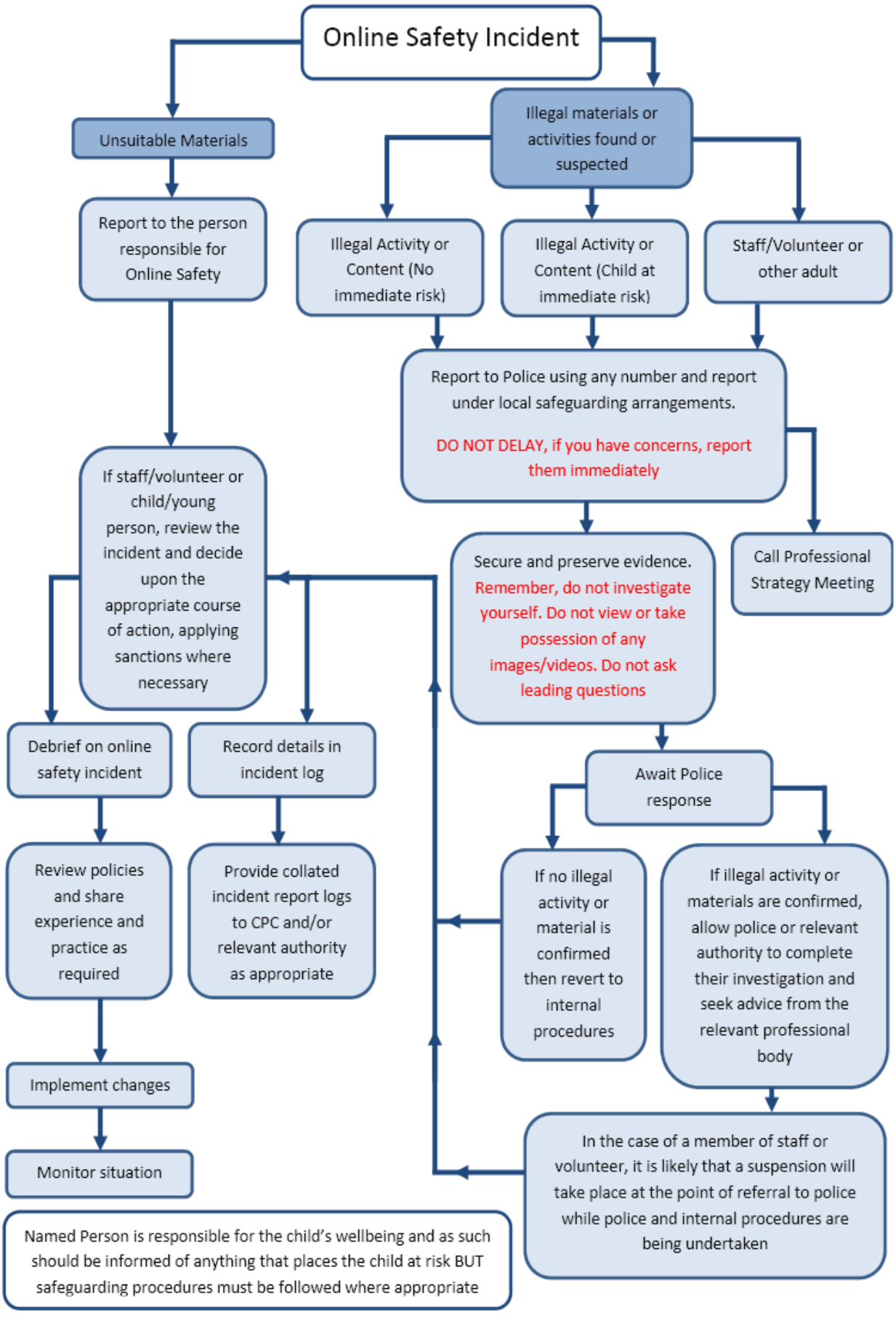
- digital and video images taken at school events
- access to parents' sections of the website, Hwb, learning platform and online learner records
- their children's personal devices in the school (where this is allowed)

Community Users:

Community users who access school systems/website/Hwb/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

In the event of a serious online safety incident, the following external persons should be informed:

- BCBC ICT Manager
- BCBC Designated Safeguarding Lead
- Police (if appropriate)


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at immediate risk)
Staff/Volunteer or other adult
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have concerns, report them immediately
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Secure and preserve evidence. Remember, do not investigate yourself. Do not view or take possession of any images/videos. Do not ask leading questions
Call Professional Strategy Meeting
Debrief on online safety incident
Record details in incident log
Await Police response
Review policies and share experience and practice as required
Provide collated incident report logs to CPC and/or relevant authority as appropriate
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
Implement changes
Monitor situation
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 safeguarding procedures must be followed where appropriate

Education and Training

Learners

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety spans across all areas of the curriculum and staff should reinforce these messages across the curriculum and not merely in 'ICT lessons'. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is planned through the ICT scheme of work as well as across a range of subjects, (e.g. ICT/PSE/DCF) and topic areas to ensure that key messages are revisited regularly.
- Key online safety messages are also reinforced through other activities such as assemblies, Safer Internet Day and PSE activities. Teachers provide a safe environment in which pupils can can influence and participate in decision-making.
- Pupils are taught to be critically aware of the materials/content they access online and that such content may be biased or controversial. Where appropriate, such discussion can help to build pupils' resilience to radicalisation.
- Pupils are taught about rights and permissions, for example understanding that photographs can be edited digitally.
- In lessons where internet use is pre-planned, it is best practice that pupils are guided to sites checked as suitable for their use. Clear processes are in place to deal with any unsuitable material that is found in internet searches.
- It is accepted that from time to time, for good educational reasons, pupils may research topics, (e.g. drugs, bullying) that may result in content being blocked. If staff feel that specific blocked content should be allowed, a request can be made to the local authority to review the content and either permanently or temporarily remove those sites from the filtered list. Any request to do so, should be auditable, with clear reasons for the need.
- If learners are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit and report any activity or outcomes of concern.
- Learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices

Parents and carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, class newsletters, school web site, Hwb,Twitter, Class Dojo
- Parents and carers evenings/sessions
- High profile events/campaigns, e.g. Safer Internet Day
- Reference to the relevant web sites/publications,

e.g. https://hwb.wales.gov.uk
- www.saferinternet.org.uk
- www.childnet.com/parents-and-carers
  (see appendix for further links/resources)

The wider community

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website and Hwb will provide online safety information for the wider community
- Supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision.

Staff/volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- The online safety co-ordinator will receive regular updates through attendance at external training events, (e.g. from Consortium/SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/phase meetings/INSET days.
- The online safety co-ordinator (or other nominated person) will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association /or other relevant organisation, (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents.

Technical – infrastructure/equipment, filtering and monitoring

The local authority provides all infrastructure support, filtering and monitoring services through an ICT Service Level Agreement. The approved local authority technical staff are fully aware of the school online safety policy/acceptable use agreements and ensure that the school infrastructure/network is as safe and secure as is reasonably possible. The Headteacher and Governing Body ensure that policies and procedures approved within this policy are implemented.

School technical systems are managed in ways that ensure that the school meets all technical safety / security requirements, with the support of the local authority.

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- Key stage 2 pupils are provided with a username and secure password by the BCBC technical support/advisor who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master/administrator" passwords for the school digital systems, used by the network manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place, (e.g. school safe)
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices. Staff and pupils are not able to download or purchase software or licences without consent from the Headteacher.
- The local authority ICT technician is responsible for installing all software and ensures that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users by the local authority. Illegal and unsuitable content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Filtering also helps to ensures children are safe from terrorist and extremist material when accessing the internet.
- Internet filter content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Where possible, BCBC technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc., from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- The provision of temporary access (e.g. trainee teachers, supply teachers, visitors) onto the school system is arranged through agreement with the local authority ICT services.
- The local authority ICT Code of Conduct determines the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school.

- An agreed policy is in place regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile technologies

All mobile technology used by pupils are provided by the school and managed by the local authority ICT department – these include: ipods, tablets, notebooks/laptops and other technology (e.g. printers) that may have the capability of utilising the school's wireless network. These devices may therefore also have access to the wider internet which may include the school learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

The majority of devices in school are used by multiple users with controlled access levels. Pupils are currently not permitted to use any personal internet-connected devices (e.g. smartphones, smart watches) during the school day whilst in the school grounds or building.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those

images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Care must be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Learners must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images.
- Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs without express informed consent.
- Written permission from parents or carers will be obtained before photographs of learners are published on the school website or used in blogs/tweets etc.
- Learners' work can only be published with the permission of the learner and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the privacy notice and lawfully processed in accordance with the conditions for processing. *(see privacy notice section in the appendix)*
- It has a data protection policy (the school has adopted the BCBC policy)
- It is registered as a data controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed/identified – the Headteacher is the Senior Information Risk Officer (SIRO). The senior admin manager and Deputy Headteacher are the information asset owners (IAOs)
- Risk assessments are carried out

- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear data protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Communications

This is an area of rapidly developing technologies and uses. The online safety group will regularly review and agree how to implement and use these technologies, taking account of pupils' age, any current guidance and considering the balance of risks/educational benefits.

Currently:

- All staff are permitted to use mobile phones for work and personal reasons, with the exception of making recordings of pupils (audio, video etc) and the storage of any personal data.
- Pupils are not permitted to use any personal internet-connected devices in school.

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

- The official school email service and Hwbmail may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report to the nominated person – in accordance with the school policy - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and learners or parents/carers (email, chat, learning platform, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. **Personal email addresses, text messaging or social media must not be used for these communications.**
- Whole class/group email addresses may be used at Foundation Phase with supervision, while learners at KS2 and above will be provided with Hwb e-mail addresses for educational use.
- Learners should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social media

With an increase in use of all types of social media for professional and personal purposes, the school has adopted the BCBC Social Media policy which sets out clear guidance for all staff to manage risk and behaviour online. Expectations for teachers' professional conduct are set out by the General Teaching Council Wales (GTCW) but all adults working in the school understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

School leaders and the Governing Body recognises that they have a duty of care to provide a safe learning environment for pupils and staff. Any staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. ll staff working at any educational establishment are expected to demonstrate a professional approach and respect for learners and their families and for colleagues and the learning setting.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to learners, parents and carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Staff are only allowed to use authorised social media accounts and to do in full recognition that:

- Social media accounts are monitoring for suitability of 'posts'

- A code of behaviour exists for users of the accounts, including systems for reporting and dealing with abuse and misuse and how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

School use of social media for professional purposes is checked regularly by the Senior Information Risk Officer and online safety group to ensure compliance with the social media, data protection, communications, digital image and video policies.

Unsuitable/inappropriate activities

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

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

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

- child sexual abuse images –The making, production or distribution of indecent images of children, contrary to The Protection of Children Act 1978
- grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.

- possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character), contrary to the Criminal Justice and Immigration Act 2008
- criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986
- pornography
- promotion of any kind of discrimination, extremism or terrorism
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- using school systems to run a private business
- using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- infringing copyright
- revealing or publicising confidential or proprietary information, (e.g. financial/personal information, databases, computer/network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- unfair usage (downloading/uploading large files that hinders others in their use of the internet)
- online gambling or personal gaming
- unlawful file sharing

Responding to incidents of misuse:

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

Illegal Incidents:

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

Other Incidents:

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

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

- Have more than one senior member of staff involved in any subsequent investigation. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by learners and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by local authority or national/local organisation (as relevant).
- Police involvement and/or action

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

In this such instance, isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

School actions:

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

Nearly all incidents of misuse by pupils would be dealt with entirely through the schools behaviour and discipline policy, except for illegal (or intended illegal) actions where it may be necessary to also refer the matter to the police.

Nearly all incidents of misuse by staff would be dealt with through the relevant disciplinary procedures, except for illegal (or intended illegal) actions where it may be necessary to also refer the matter to the police.

END OF DOCUMENT