"Opening doors to the future"

CYNGOR BWRDEISTREF SIROL MERTHYR TUDFIL

MERTHYR TYDFIL COUNTY BOROUGH COUNCIL

GREENFIELD SCHOOL POLICY

2022

Online Safety

Rhiannon Stephens Davies, Head Teacher.
Rachel Faulkner, Deputy Head - Standards
Carol Conway, Deputy Head - Wellbeing

' Opening Doors To The Future '
' Agordrysaui'rdyfodol'

Date	**Author**
Feb 2022	Kira John

MONOTORING THE POLICY

This policy will be reviewed bi-annually unless change of circumstances or legislation requires it to be amended earlier.

Signed: ………………………………………………………………………………………….. Date: …………………………………………………….

Headteacher

Signed: ………………………………………………………………………………………….. Date: …………………………………………………….

Chair of Governors

MISSION STATEMENT

‘ OPENING DOORS TO THE FUTURE ‘

At Greenfield School we strive to:

- To provide a positive learning environment, for all children to maximise their learning potential.
- To promote achievement and recognise all effort.
- To develop self-esteem and confidence.
- To help pupils understand the world in which they live and acquire relevant knowledge and skills.
- To encourage respect and tolerance for other religions and lifestyles.

Background / Rationale

The use of exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

The improper or unsafe use of technology can present challenges to children, young people, volunteers and staff.

Some of the potential risks could include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to exploitation and abused by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual’s consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Blackmail involving threats to life, dignity and violence
- Poor or inappropriate supervision of Internet access leading to the viewing of harmful or inappropriate images
- Risk of sexual exploitation

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils’ resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

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

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The 2011 Education Act increased these powers with regards to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published behaviour policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that takes place out of school.

Roles and Responsibilities

In order to ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns and misuse as soon as these become apparent. While this will be a team effort, the following sections outline 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 Governing Body 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
- regular monitoring of online safety incident logs
- regular monitoring of filtering change control logs (where possible)
- reporting to relevant governors/sub-committee/meeting

Head teacher and senior leaders:

- The head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety may be delegated to the online safety co-ordinator.
- The head teacher and members of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The head teacher/senior leaders are responsible for ensuring that the online safety co-ordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- The head teacher/senior leaders 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.
- The head teacher/senior leaders will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

- Lead the Online Safety Group
- Work closely on a day-to-day basis with the Designated Safeguarding Person (DSP), where these roles are not combined
- Take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- Have a leading role in establishing and reviewing the school online safety policies/documents
- Promote an awareness of and commitment to online safety education across the school and beyond
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned and embedded
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- Receive reports of online safety incidents6 and create a log of incidents to inform future online safety developments
- Provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- Liaise with (school/local authority) technical staff, pastoral staff and support staff (as relevant)
- Meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- Attend relevant governing body meetings/groups
- Report regularly to head teacher/senior leadership team.
- Liaises with the local authority/relevant body

Teaching and Support Staff

Are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- They understand that online safety is a core part of safeguarding
- They have read, understood and signed the staff acceptable use agreement (AUP)
- They immediately report any suspected misuse or problem to ICT lead for investigation/action, in line with the school safeguarding procedures
- All digital communications with learners and parents/carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They supervise and 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 processes are in place for dealing with any unsuitable material that is found in internet searches
- Where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the Live-streaming and video-conferencing: safeguarding principles and practice guidance
- They have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc

- They model safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Safeguarding Designated Person

The Safeguarding Designated Person is trained in Online Safety issues and is aware of the potential for serious safeguarding issues that could arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Curriculum Leads

Curriculum leads will work with the online safety lead to develop a planned and coordinated online safety education programme. This will be provided through:

- A discrete programme
- The DCF
- Personal & Social Education/Sex and Relationships education
- Assemblies and pastoral programmes
- Through relevant national initiatives and opportunities. E.g. Safer Internet Day/ Anti Bullying Week.

E-Safety Group

Members of the e-Safety Group will assist the *e-Safety Coordinators* with:

- The production / review / monitoring of the school e-Safety policy / documents
- The production / review / monitoring of the school filtering policy (if possible and if the school chooses to have one) and requests for filtering changes
- Mapping and reviewing the e-Safety curricular provision – ensuring relevance, breadth and progression
- Monitoring network / internet / incident logs where possible
- Consulting stakeholders – including parents / carers and the pupils about the e-Safety provision

Learners:

- Are responsible for using the schools 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 schools 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
- 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 AUP before being provided with access to school systems.

Online Safety Policy

The school Online Safety Policy:

- Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- Allocates responsibilities for the delivery of the policy
- Is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- Establishes guidance for staff in how they can use digital technologies responsibly, protecting themselves and the school and how they can use this understanding to help safeguard learners in the digital world
- Describes how the school will help prepare learners to be safe and responsible users of online technologies
- Establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- Is supplemented by a series of related acceptable use agreements
- Is made available to staff at induction and through normal communication channels
- Is published on the school website.

Acceptable Use

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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					X
	grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003					X
	possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character), contrary to the Criminal Justice and Immigration Act 2008					X
	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					X

	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	promotion of extremism or terrorism				X	
	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				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act (1990): • Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)						X
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information, (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Online gaming (educational)		X				
Online gaming (non educational)					X	
Online gambling					X	
Online shopping/commerce				X		
File sharing				X		
Use of social media				X		
Use of messaging apps					X	
Use of video broadcasting, e.g. YouTube				X		

	Staff and other adults				Pupils		
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed with staff permission	Not Allowed
Mobile phones may be brought to school	X					X	
Use of mobile phones in lessons				X			X
Use of mobile phones in social time	X					X	
Taking photos on mobile phones/cameras				X			X
Use of other mobile devices, e.g. tablets, gaming devices	X					X	
Use of personal e-mail addresses in school, or on school network				X			X
Use of school e-mail for personal e-mails				X			X
Use of messaging apps	X						X
Use of social media	X						X
Use of blogs	X					X	

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

- The official school e-mail service may be regarded as safe and secure and is monitored. Users should be aware that e-mail communications are monitored. *Staff and learners should therefore use only the school e-mail service to communicate with others when in school, or on school systems (e.g. by remote access)*
- Users must immediately report to the ICT Lead/ SMT – 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 (e-mail, chat, learning platform, etc.) must be professional in tone and content. *These communications may only take place on official (monitored) school systems. Personal e-mail addresses, text messaging or social media must not be used for these communications*

- 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 digital citizenship and the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official e-mail addresses should be used to identify members of staff.

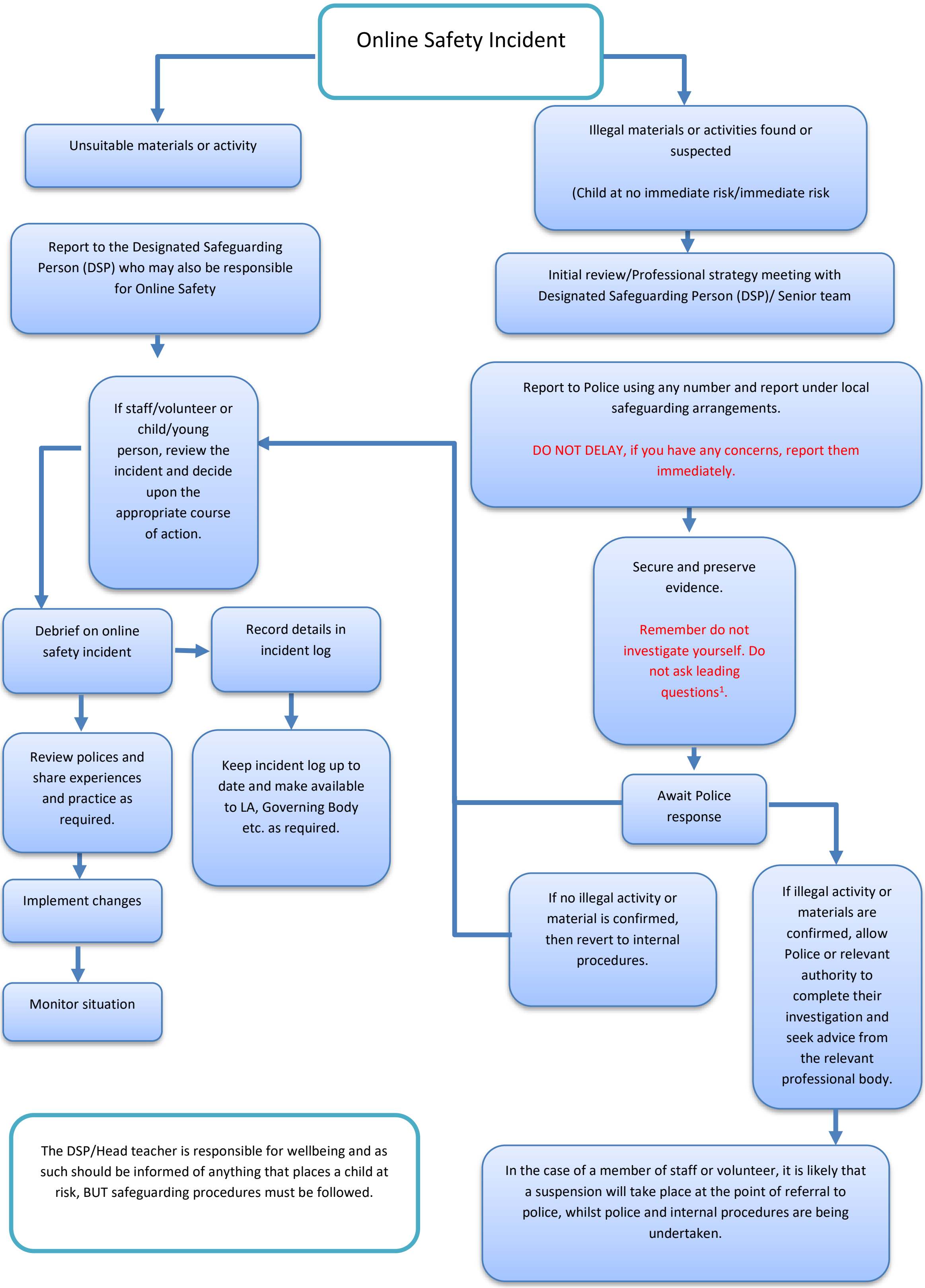
Reporting and responding

The school will take all reasonable precautions to ensure online safety for all school users, but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the school community will be made aware of the need to immediately report online safety issues/incidents
- Reports will be dealt with as soon as is practically possible once they are received
- The Designated Safeguarding Person, Online Safety Lead and other responsible staff have appropriate skills and training to deal with the various risks related to online safety
- If there is any suspicion that the incident involves child abuse images, any other illegal activity or the potential for serious harm, the incident must be escalated through the normal school safeguarding procedures and the police informed. In these circumstances any device involved should be isolated to support a potential police investigation. In addition to child abuse images such incidents 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.
- Any concern about staff misuse will be reported immediately to the ICT Lead/ SMT, unless the concern involves the ICT Lead/ SMT, in which case the complaint is referred to the Chair of Governors and the local authority
- As long as there is no suspected illegal activity devices may be checked using the following procedures:
    - One or more senior members of staff should be involved in this process. 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 (should illegal activity be subsequently suspected). 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 incident form (except in the case of images of child sexual abuse – see above).
    - 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 (as relevant)
    - police involvement and/or action
- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- There are support strategies in place e.g. peer support for those reporting or affected by an online safety incident
- Incidents should be logged using 'My Concern' headed with online Safety.
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP; Keeping safe online on Hwb
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- Learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
- *staff, through regular briefings*
- *learners, through assemblies/lessons*
- *parents/carers, through newsletters, school social media, website*
- *governors, through regular safeguarding updates*
- *local authority/external agencies, as relevant*

The flowchart below should be followed to support the decision-making process for dealing with online safety incidents.



Online Safety Incident

Unsuitable materials or activity

Report to the Designated Safeguarding Person (DSP) who may also be responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action.

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Keep incident log up to date and make available to LA, Governing Body etc. as required.

Implement changes

Monitor situation

Illegal materials or activities found or suspected

(Child at no immediate risk/immediate risk

Initial review/Professional strategy meeting with Designated Safeguarding Person (DSP)/ Senior team

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not ask leading questions[1].

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, whilst police and internal procedures are being undertaken.

The DSP/Head teacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

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. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Learner actions

Incidents	Refer to class teacher	Refer to SMT	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Issue a warning	Further sanction, e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal	X	X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons.	X				X			X	
Unauthorised use of mobile phone/digital camera/other mobile device.	X	X						X	
Unauthorised use of social media/messaging apps/personal e-mail.	X	X						X	
Unauthorised downloading or uploading of files.	X	X			X		X	X	
Allowing others to access school network by sharing username and passwords.	X	X					X	X	
Attempting to access or accessing the school network, using another learners' account.	X	X					X	X	
Attempting to access or accessing the school network, using the account of a member of staff.	X	X	X		X	X	X	X	
Corrupting or destroying the data of other users.	X	X	X		X	X	X	X	
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.	X	X	X		X	X	X	X	
Continued infringements of the above, following previous warnings or sanctions.	X	X	X	X	X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X	X	X	X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system.	X	X			X		X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X	X		X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material.	X	X	X	X	X	X	X	X	X

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X	X	X	X	X	X	X	X	X

Staff Actions

Incidents	Refer to line manager/ SMT	Refer to Headteacher	Refer to local authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal	x	x	x	x	x	x	x	x
Inappropriate personal use of the internet/social media/personal e-mail	x	x			x	x		
Unauthorised downloading or uploading of files.	x	x			x			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	x	x	x		x	x		
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	x	x	x		x	x		
Deliberate actions to breach data protection or network security rules.	x	x	x		x	x		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x	x		x	x		
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.	x	x	x			x		
Using personal e-mail/social networking/messaging to carrying out digital communications with learners and parents/carers	x	x				x		
Actions which could compromise the staff member's professional standing	x	x	x	x	x	x	x	
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	x	x	x		x	x	x	

Using proxy sites or other means to subvert the school’s filtering system.	x	x			x			
Accidentally accessing offensive or pornographic material and failing to report the incident.	x	x	x	x	x	x		
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x	x	x	x
Breaching copyright or licensing regulations.	x	x	x	x	x	x	x	x
Continued infringements of the above, following previous warnings or sanctions.	x	x	x	x	x	x	x	x

Education

Online Safety Education Programme

While 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 develop their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. 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 across all year groups and a range of subjects, (e.g. DCF/PSE/RSE/Health and Well-being) and topic areas and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- It incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- The programme will be accessible to learners at different ages and abilities
- Learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. NB additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet
- 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

- In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other nominated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- The online safety education programme will be regularly audited and evaluated to ensure the quality of learning and outcomes.

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 and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process
- The training will be an integral part of the school's annual safeguarding and data protection training for all staff
- All new staff will 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 ICT lead and Designated Safeguarding Person (or other nominated person) will receive regular updates through attendance at external training events
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions:

- Hwb training – Online safety for governors
- Attendance at training provided by the local authority or other relevant organisation (e.g. SWGfL)
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training will be made available to the Online Safety Governor.

The school will provide all governors with an Hwb account in order to use the secure tools and services available e.g. Microsoft Outlook, Teams etc as well as appropriate application training. This negates the need for governors to use personal email accounts, thereby reducing the risk to data.

Families

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 seek to provide information and awareness to parents and carers through:

- Regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- Regular opportunities for engagement with parents/carers on online safety issues through awareness workshops/parent/carer evenings etc
- The learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- Letters, newsletters, website, learning platform, Hwb
- High profile events/campaigns e.g. Safe Internet Day
- Reference to the relevant web sites/publications, e.g. Hwb Keeping safe online, www.saferinternet.org.uk/ www.childnet.com/parents-and-carers
- Sharing good practice with other schools in clusters and or the local authority

Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering

- The school filtering policies are agreed by MTCBC and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- The school manages access to content across its systems for all users. The filtering provided meets the standards defined in the Welsh Government Recommended web filtering standards for schools and the UK Safer Internet Centre Appropriate filtering.
- Internet access is filtered for all users
- Illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated (n.b. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet
- There are established and effective routes for users to report inappropriate content
- There is a clear process in place to deal with requests for filtering changes
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different groups of users: staff/learners, etc.)
- There is an appropriate and balanced approach to providing access to online content according to role and/or need
- Filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
- Where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- The system manages access to content through non-browser services (e.g. apps and other mobile technologies)

If necessary, the school will seek advice from, and report issues to MTCBC ICT team.

Monitoring

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through:

- Physical monitoring (adult supervision in the classroom)
- Internet use is logged, regularly monitored and reviewed
- Filtering logs are regularly analysed and breaches are reported to senior leaders
- Pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems

Users are made aware, through the acceptable use agreements, that monitoring takes place.

Technical Security

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling are securely located and physical access restricted
- There are rigorous and verified back-up routines, including the keeping of copies off-site or in the cloud, (this is good practice in helping to prevent loss of data from ransomware attacks)
- All users have clearly defined access rights to school technical systems and devices.
- All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details. Sharing of passwords or ID and passwords could lead to an offence under the Computer Misuse Act 1990. Users must immediately report any suspicion or evidence that there has been a breach of security
- All school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by the ICT lead or ICT Technician who will keep an up to date record of users and their usernames
- Passwords should be long. Good practice highlights that passwords over 12 characters in length are more difficult to crack. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length is more secure than any other special requirements such as uppercase/lowercase letters, number and special characters. Users should be encourage to avoid using sequential or chronological numbers within their passwords. Passwords/passphrases should be easy to remember, but difficult to guess or crack
- Records of learner usernames and passwords can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- ICT Lead or ICT technician is responsible for ensuring that software licence logs are accurate and up-to-date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- An appropriate system my concern or online cyber log is in place for users to report any actual/potential technical incident/security breach to the relevant person
- 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.

- An agreed policy is in place for the provision of temporary access of 'guests', (e.g. trainee teachers, supply teachers, visitors) onto the school systems
- An agreed policy is in place regarding 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 that allows staff to/forbids staff from downloading executable files and installing programmes on school devices
- An agreed policy is in place regarding the use of removable media (e.g. 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. (See GDPR policies)

Mobile technologies

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

A range of mobile technology implementations is possible and used when needed.

Social media

With an increase in use of all types of social media for professional and personal purposes, this policy that sets out clear guidance for staff to manage risk and behaviour online is essential.

Expectations for teachers' professional conduct are set out by the General Teaching Council Wales (GTCW) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, 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. All staff working at any educational establishment are expected to follow the professional conduct set out by the General Teaching Council Wales (GTCW) and respect learners, their families, colleagues and the school.

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

- Ensuring that personal information is not published
- Education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

- Guidance for learners, parents/carers

School staff should ensure that:

- No reference should be made in social media to learners, parents/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
- They act as positive role models in their use of social media
- Staff should not be friends with pupils on any social media sites

Personal use

- Personal communications are those made via 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, the school will 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 and in guidance with the LA
- When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Group to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

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/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying 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 live-streaming or video-conferencing, governing bodies, head teachers and staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the Live-streaming and video-conferencing: safeguarding principles and practice guidance
- 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, storage, distribution and publication of those images. Staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes
- Care should 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 social media, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes
- Parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- Images will be securely stored on the school network in line with the school retention policy
- Learners' work can only be published with the permission of the learner and parents/carers

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters
- SCHOOP
- Seesaw

The school website is managed/hosted by the ICT Lead. The school ensures that good practice has been observed in the use of online publishing e.g. use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is no risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected and full names are not published.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school:

- Has a Data Protection Policy
- Implements the data protection principles and is able to demonstrate that it does so
- Has paid the appropriate fee to the Information Commissioner's Office (ICO)
- Has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- Has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- The Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- Has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- Information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- Will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this
- Data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- Provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- Has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
- Carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- Has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- Understands how to share data lawfully and safely with other relevant data controllers.
- Has clear and understood policies and routines for the deletion and disposal of data
- Reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- As a maintained school, has a Freedom of Information Policy which sets out how it will deal with FOI requests

- Provides protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

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

- Data will be encrypted and password protected.
- Device will be password protected.
- Device will be protected by up to date virus and malware checking software
- Data will be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

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
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- Can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- Only use encrypted mobile devices (including USBs) for personal data, particularly when it is about children
- Will not transfer any school personal data to personal devices. Procedures should be in place to enable staff to work from home (i.e. VPN access to the school network, or a work laptop provided).
- 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, a secure email account (where appropriate), and secure password protected devices.