*Ysgol Mynydd Bychan*



E-Safety Policy

**17/02/22**

**Development / Monitoring / Review of this Policy**

4

This e-safety policy has been developed by Ysgol Mynydd Bychan’s Digital Leaders Groupmade up of: *(*

*• Iolo Williams (Deputy, ICT Co-ordinator)*

*• Non Bullen, Lois Williams (Teachers)*

*• Natalie Hill*

*• Governors*

*• Parents and Carers*

*• Pupils*

**Schedule for Development / Monitoring / Review**

5

|  |  |
| --- | --- |
| This e-safety policy was approved by the Governing Body *on:* | 17/02/22 |
| The implementation of this e-safety policy will be monitored by the: | Ysgol Mynydd Bychan’s Digital Leaders Group |
| Monitoring will take place at regular intervals: | September |
| The *Governing Body* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals: | *Spring Term* |
| The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: | *Spring Term* |
| Should serious e-safety incidents take place, the following external persons / agencies should be informed: | Richard Clement –E-Safety Manager, Cardiff Education Authority - (or his deputy, Sarah Dawson, in his absence) |

The school will monitor the impact of the policy using:

*•* Logs of reported incidents

• Monitoring logs of internet activity (including sites visited)

• Internal monitoring data for network activity

• Surveys / questionnaires of

• students / pupils

• parents / carers

• staff

6

**Scope of the Policy**

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the schoolsite 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 outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard 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 schoolwill deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate e-safety behaviour that take place out of school.

**Roles and Responsibilities**

7

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

**Governors:**

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governorsreceiving regular information about e-safety incidents and monitoring reports. A member of the Governing Bodyhas taken on the role of *E-Safety Governor* . The role of the E-Safety Governorwill include:

*•* regular meetings with the E-Safety Co-ordinator

• regular monitoring of e-safety incident logs

• regular monitoring of filtering / change control logs

• reporting to relevant Governors

**Headteacher and Senior Leadership Team:**

• **The *Headteacher* has a duty of care for ensuring the safety (including e-safety) of members of the school community**, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.

• **The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.** (see flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant *Local Authority HR / other relevant body* disciplinary procedures).

*•* The Headteacher and Senior Leadership Team are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

*•* The Headteacher and Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

*•* The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

**E-Safety Coordinator:**

• leads the e-safety committee

• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents

• ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

• provides training and advice for staff

• liaises with the Local Authority / relevant body

• liaises with school technical staff

• receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,

• meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs

• attends relevant meeting / committee of Governors

• reports regularly to Senior Leadership Team

**Network Manager / Technical staff:**

**Teaching and Support Staff**

are responsible for ensuring that:

**• they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices**

**• they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)**

**• they report any suspected misuse or problem to the Headteacher Senior Leadership Team ; E-Safety Coordinator for investigation / action / sanction**

**• all digital communications with students / pupils / parents / carers should be on a professional level** and only carried out using official school systems

• e-safety issues are embedded in all aspects of the curriculum and other activities

• pupils understand and follow the e-safety and acceptable use policies

• pupils 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 pupils 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

**Safeguarding Officer**

should be trained in e-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 on-line contact with adults / strangers

• potential or actual incidents of grooming

• cyber-bullying

**Digital Leaders Group**

The Digital Leaders Group provides a consultative group that has wide representation from the schoolwith responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. Depending on the size or structure of the school this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the Digital Group will assist the E-Safety Officer with:

• the production / review / monitoring of the school e-safety policy / documents.

• the production / review / monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes*.*

*•* mapping andreviewing the e-safety curricular provision – ensuring relevance, breadth and progression

*•* monitoring network / internet / incident logs

*•* consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision

*•* monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils:

**• are responsible for using the school’s digital technology systems in accordance with the Pupil 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 e-safety practice when using digital technologies out of school and realise that the *school’s*  E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Theschoolwill take every opportunity to help parents understand these issues through parents’ evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-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 / VLE and on-line pupil records

• their children’s personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems / website / VLE as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

11

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of  *pupils* in e-safety is therefore an essential part of the school’s e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

**E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:**

**• A planned e-safety curriculum should be provided as part of digital competence / PHSE / other lessons and should be regularly revisited**

**• Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities**

**• Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**

**• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**

*• Pupils should be helped to understand the need for the pupil 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 pupils 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 pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*

*• It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the LEA 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.*

Education – parents / carers

Many parents and carers have only a limited understanding of e-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 on-line 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, newsletters, web site, VLE*

*• Parents / Carers evenings / sessions*

*• High profile events / campaigns eg Safer Internet Day*

*• Reference to the relevant web sites*

Education – The Wider Community

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

* *Providing family learning courses in use of new digital technologies, digital literacy and e-safety*
* *E-Safety messages targeted towards grandparents and other relatives as well as parents.*
* *The school / academy website will provide e-safety information for the wider community*
* *Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision*

Education & Training – Staff / Volunteers

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

• **A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.**

 *It is expected that some staff will identify e-safety as a training need within the performance management process.*

**• All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.**

*• The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.*

*• This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.*

*• The E-Safety Coordinator / Officer will provide advice / guidance / training to individuals as required.*

Training – Governors

**Governors / Directors should take part in e-safety training / awareness sessions**, with particular importance for those who are members of any sub committee involved in technology / e-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 (eg SWGfL).

• Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

See Appendix A

**Bring Your Own Device (BYOD)**

If a pupil brings a mobile phone to school for some purpose (eg to contact parents on the way home at the end of the day), they must be kept locked away. the Headteacher's room or their classroom. It is the pupil's responsibility to ensure that the phone is handed to the Headteacher / teacher and collected at the end of the day.

Progress Step 3 pupils can bring their own mobile device to the classroom if a prior arrangement has been made with one of the teachers or the Head teacher and if there is a valid reason to do so e.g. show a piece of work. When the device in question is not being used in class, it should be ensured that it is locked in the Headteacher's room.

Owners of devices that carry them to school do so at their own risk, and users and their parents / carers are solely responsible for the costs of any loss or damage resulting from their use of any device at school.

The school accepts no responsibility or liability for lost, stolen or damaged devices at school, or in the conduct of school-organized activities.

The school accepts no responsibility for defects in any device due to changes made to the device while on the school network.

The school recommends that devices should be easily identifiable and have a protective box to protect when transporting them around the school. Access devices or personal identification number should be placed on personal devices to help protect them.

The school is not responsible for the maintenance of users' personal devices, such as charging any device, installing software updates or resolving hardware problems.

Users are expected to act responsibly, securely and respectfully in accordance with current Acceptable Use Agreements.

When any mobile device is in the classroom, make sure that the following rules are followed:

• The screen must be visible at all times i.e. face up on the desk.

• Teachers and / or students must be allowed access to any pupil's device.

• Cannot take photos or videos without the teacher's authorization

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils 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 pupils 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 eg 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 *pupils* 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 should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*

• *Pupils must not take, use, share, publish or distribute images of others without their permission*

• *Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.*

• *Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.*

• *Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website*

• *Pupil’s work can only be published with the permission of the pupil and parents or carers.*

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2020 which states that personal data must be:

• Fairly and lawfully processed

• Processed for limited purposes

• Adequate, relevant and not excessive

• Accurate

• 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”.**
* **It has a Data Protection policy**
* **It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)**
* 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 be password protected **•** the device must offer approved virus and malware checking software

16

**•** 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

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

|  |  |  |
| --- | --- | --- |
|  | Staff & other adults | Pupils |
| Communication Technologies | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to school |  |  |  |  |  |  |  |  |
| Use of mobile phones in lessons |  |  |  |  |  |  |  |  |
| Use of mobile phones in social time |  |  |  |  |  |  |  |  |
| Taking photos on mobile phones / cameras |  |  |  |  |  |  |  |  |
| Use of other mobile devices eg tablets, gaming devices  |  |  |  |  |  |  |  |  |
| Use of personal email addresses in school, or on school network |  |  |  |  |  |  |  |  |
| Use of school email for personal emails |  |  |  |  |  |  |  |  |
| Use of messaging apps |  |  |  |  |  |  |  |  |
| Use of social media  |  |  |  |  |  |  |  |  |
| Use of blogs |  |  |  |  |  |  |  |  |

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

**• The official *school* email service may be regarded as safe and secure and is monitored.****Users should be aware that email communications are monitored.**  *Staff and pupils should therefore use only the school email service to communicate with others when in school, or on schoolsystems (eg by remote access).*

**• 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 pupils or parents / carers (email, chat 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 Progress step 1 and 2, while pupils at Progress Step 3 and above will be provided with individual school email addresses for educational use*

*• Pupils should be taught about e-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 - Protecting Professional Identity

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

All schools and local authorities have a duty of care to provide a safe learning environment for pupils 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, 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. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

* Training to include: 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 pupils, 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.

The *school’s* use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

School Twitter account

If a message is to be placed on the school's Twitter account, it must be ensured on a secure device and that the user 'logs out' at the end of the session. If pictures of pupils are to be included as part of the message, parents / carers must have given their consent for this to happen as part of the Acceptable Use Agreement.

Unsuitable / inappropriate 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 school or outside school when using school equipment or systems. The school policy restricts usage as follows:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| User Actions18 | 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  |  |
| **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  |  |
| **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 (eg 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 |  |
| **On-line gaming (educational)** |  |  |  |  |  |
| **On-line gaming (non educational)** |  |  |  |  |  |
| **On-line gambling** |  |  |  |  |  |
| **On-line shopping / commerce** |  |  |  |  |  |
| **File sharing** |  |  |  |  |  |
| **Use of social media**  |  |  |  |  |  |
| **Use of messaging apps** |  |  |  |  |  |
| **Use of video broadcasting eg Youtube**19 |  |  |  |  |  |

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 or 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 / volunteer 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 young people 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
* other criminal conduct, activity or materials
* **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 child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school / academy 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:

|  |  |
| --- | --- |
| Students / Pupils | Actions / Sanctions  |
| Incidents: | Refer to class teacher / tutor | Refer to Headteacher | Refer to Deputy | Refer to Police | Refer to technical support staff for action re filtering / security etc | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction eg detention / exclusion |
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** |  | X | X | X |  |  |  |  |  |
| Unauthorised use of non-educational sites during lessons |  |  |  |  |  |  |  |  |  |
| Unauthorised use of mobile phone / digital camera / other mobile device |  |  |  |  |  |  |  |  |  |
| Unauthorised use of social media / messaging apps / personal email |  |  |  |  |  |  |  |  |  |
| Unauthorised downloading or uploading of files |  |  |  |  |  |  |  |  |  |
| Allowing others to access school network by sharing username and passwords |  |  |  |  |  |  |  |  |  |
| Attempting to access or accessing the school / academy network, using another pupil’s account |  |  |  |  |  |  |  |  |  |
| Attempting to access or accessing the school network, using the account of a member of staff |  |  |  |  |  |  |  |  |  |
| Corrupting or destroying the data of other users |  |  |  |  |  |  |  |  |  |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature |  |  |  |  |  |  |  |  |  |
| Continued infringements of the above, following previous warnings or sanctions |  |  |  |  |  |  |  |  |  |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school |  |  |  |  |  |  |  |  |  |
| Using proxy sites or other means to subvert the school’ filtering system |  |  |  |  |  |  |  |  |  |
| Accidentally accessing offensive or pornographic material and failing to report the incident |  |  |  |  |  |  |  |  |  |
| Deliberately accessing or trying to access offensive or pornographic material |  |  |  |  |  |  |  |  |  |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act21 |  |  |  |  |  |  |  |  |  |

|  |  |
| --- | --- |
| Staff | Actions / Sanctions  |
| Incidents: | Refer to line managerr | Refer to Headteacher | Refer to Local Authority / HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc | Warning | Suspension | Disciplinary action |
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** |  | X | X | X |  |  |  |  |
| Inappropriate personal use of the internet / social media / personal email |  |  |  |  |  |  |  |  |
| Unauthorised downloading or uploading of files |  |  |  |  |  |  |  |  |
| 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 |  |  |  |  |  |  |  |  |
| Careless use of personal data eg holding or transferring data in an insecure manner |  |  |  |  |  |  |  |  |
| Deliberate actions to breach data protection or network security rules |  |  |  |  |  |  |  |  |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software |  |  |  |  |  |  |  |  |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature |  |  |  |  |  |  |  |  |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils |  |  |  |  |  |  |  |  |
| Actions which could compromise the staff member’s professional standing  |  |  |  |  |  |  |  |  |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school / academy  |  |  |  |  |  |  |  |  |
| Using proxy sites or other means to subvert the school’s filtering system |  |  |  |  |  |  |  |  |
| Accidentally accessing offensive or pornographic material and failing to report the incident |  |  |  |  |  |  |  |  |
| Deliberately accessing or trying to access offensive or pornographic material |  |  |  |  |  |  |  |  |
| Breaching copyright or licensing regulations |  |  |  |  |  |  |  |  |
| Continued infringements of the above, following previous warnings or sanctions |  |  |  |  |  |  |  |  |

22

Appendix

Appendix One – Atodiad 1A – (Cardiff LEA)

**Technical**

The control, management and monitoring of infrastructure and equipment (internet filtering system and network resources; data; shares; services and software) play a key role in e-safety.

This section of the document outlines schools’ and individuals’ responsibilities when setting up, connecting and using ICT equipment.

Existing policies and documents outlining conditions of use are in operation, they support and supplement the information and good practice detailed below.

**Supporting Documents:**

* Schools Broadband Terms and Conditions
* E-mail Acceptable Use Policy
* Internet Acceptable Use Policy
* Schools Remote Working Policy
* School’s Responsibilities –ICT Service Level Agreement

**Context**

All schools are connected to a shared network, provided for schools. Clients, Servers and Users connecting to the network are administered by the ICT Department. Each school has access to a managed wireless and wired network, a filtered internet connection and firewall protection. These services are configured with policies and controls to prevent misuse, malicious attack and to ensure the protection and safety of our data, staff and learners.

The managed service is subject to conditions of use, as outlined in the Broadband Terms and Conditions document, and the Schools’ Responsibilities section of the ICT Support SLA.

It is the schools’ responsibility to ensure that users of ICT systems and equipment are aware of, have access to and have signed the appropriate Acceptable Use Policies.

Where schools have different ICT infrastructures (or elements not maintained by the ICT Department) then it is the school’s responsibility to ensure:

* Standards of security and controls implemented will need to be equivalent to those outlined in this and other supporting policy documents.
* The security of the schools’ Shared Network should not be jeopardised or undermined

In all instances, Schools should name those individuals responsible for upholding the policy(s) implementation and compliance.

**Connections to the Schools’ Network**

* Equipment connected to the Shared Schools Network should be owned by the school and in line with the limitations set out in the Schools ICT Support SLA
* Antivirus: In line with the Schools Broadband Terms and Conditions, it is the school’s responsibility to ensure workstations and other devices are protected by up to date virus software.
* Appropriate security measures are in place to protect the servers, networking equipment, work stations, hand held devices, etc from accidental or malicious attempts which might threaten the security of the school systems and data. These measures should not be circumvented or attempts made to do so.

**Internet Filtering**

* The school uses and supports the managed filtering service provided by ICT Department
* Any filtering issues should be reported immediately to the ICT Department (Schools ICT) Helpdesk.
* The School’s own Internet Acceptable Use Policy uses the whole of the ICT Internet Policy as a baseline – adding policy statements applicable to the local context if needed.
* In accordance with the Internet Acceptable Use Policy, school ICT technical or ICT staff may monitor and record the activity of users on the school ICT systems. Users are made aware of this in the Acceptable Use Policy.
* School does have the power to block / unblock specific websites at the School’s own discretion via the Swurl service. However, this will only be done by the E-Safety Co-Ordinator and will only happen after further external advice has been taken regarding the potential risks of undertaking the proposed action.

**Access, Controls and Restrictions**

* Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

13

* All users will have clearly defined access rights to school ICT systems
* Servers, wireless systems and cabling must be securely located and with physical access restricted
* Regular reviews and audits of the safety and security of school ICT systems should be undertaken
* Schools should limit the potential for data loss, Data Security Incidents and the spread of malicious software by controlling the use of removable media.
* Removable media should be encrypted and allocated to individual users.
* Removable media should not be used to transfer data between the Administrative and Curriculum networks
* User may only be granted access to the network/system/software/data resources for which they have a requirement to use.
* An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, visitors) onto the school system.

**Information Security**

* School owned portable ICT equipment should be used in accordance with the Schools Remote Working Policy.
* Personal data about individual staff and learners cannot be sent over the internet (e-mail, attachment or other upload) or taken off the school site unless safely encrypted or otherwise secured.
* The School’s own Remote Working Policy Acceptable Use Policy uses the whole of the ICT Internet Policy as a baseline – adding policy statements applicable to the local context if needed.
* Information Security Incidents should be logged with the Information Security Officer at the earliest opportunity.

The School’s own E-mail Acceptable Use Policy uses the whole of the ICT Internet Policy as a baseline – adding policy statements applicable to the local context if needed.

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

<http://www.swgfl.org.uk/Staying-Safe/Creating-an-E-Safety-policy>

23

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School E-Safety Policy Template and of the 360 degree safe E-Safety Self Review Tool:

• Members of the SWGfL E-Safety Group

• Avon and Somerset Police

• Representatives of SW Local Authorities

• Plymouth University Online Safety

• NEN / Regional Broadband Grids

Copyright of these Template Policies is held by SWGfL. Schools / Academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (esafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is

accurate, as at the date of publication in October 2013. However, SWGfL can not

guarantee it’s accuracy, nor can it accept liability in respect of the use of the material.

© SWGfL 2013