



Coed Y Brain Primary School



Online Safety

Let's
BELIEVE *to* **ACHIEVE**



 Ambitious & Capable

 Healthy & Confident

 Ethical & Informed

 Enterprising & Creative

Coed Y Brain Primary School
Online Safety Policy



This Online Safety policy has been developed by staff, pupils and governors at Coed Y Brain Primary School. This policy should be read alongside CYB policies and procedures on child protection and safeguarding, anti bullying and Distance/Blended Learning.

Purpose

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices*
- provide staff and volunteers with the overarching principles that guide our approach to online safety*
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.*

Legal framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in Wales

Summaries of the key legislation and guidance are available on: • online abuse • bullying • child protection
See <https://learning.nspcc.org.uk/> for useful links.

We believe that:

- children and young people should never experience abuse of any kind*
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.*

We recognise that:

- the online world provides everyone with many opportunities; however it can also present risks and challenges*
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online*
- we have a responsibility to help keep children and young people safe online, whether or not they are using CYB's network and devices*
 - working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety*
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse*

We will seek to keep children and young people safe by:

- *appointing an online safety coordinator – Mr Andrew Morgan*
- *providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults*
- *supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others*
- *supporting and encouraging parents and carers to do what they can to keep their children safe online*
- *developing an online safety agreement for use with young people and their parents or carers*
- *developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person*
- *reviewing and updating the security of our information systems regularly*
- *ensuring that user names, logins, email accounts and passwords are used effectively*
- *ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate*
- *ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given*
 - *providing supervision, support and training for staff and volunteers about online safety*
- *examining and risk assessing any social media platforms and new technologies before they are used within the organisation*

Roles and Responsibilities

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

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports via termly Headteacher reports to Governing Body.

Head teacher and SLT

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, through the day to day responsibility for online Safety. The Headteacher and Safeguarding Leads 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. (See flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority disciplinary procedures).

Network Manager

Local Authority Network Manager is responsible for ensuring:

- *that the school’s technical infrastructure is secure and is not open to misuse or*

malicious attack

- *the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant*
- *CYB has a Service Level Agreement with CCBC to provide safe access as far as possible*

Teaching and Support Staff

Are responsible for ensuring that:

- *they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices*
- *they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)*
- *they report any suspected misuse or problem to the Headteacher and Online Safety Co-ordinator 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*
- *online safety issues are embedded in all aspects of the curriculum and other activities*
- *students / pupils understand and follow the Online Safety Policy and acceptable use policies*
- *students / 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*

Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / 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*
- *Online-bullying*

Pupils:

- *are responsible for using the school 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 online-bullying.*
- *should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school*

Parents / 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. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- *digital and video images taken at school events*
- *access to parents' sections of the website / Learning Platform and on-line pupil records*
- *their children's personal devices in the school (where this is allowed)*

Policy Statements

Education – Students / 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 online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build 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 should be provided as part of Computing / PHSE / other lessons and should be regularly revisited*
- *Key online safety messages should be reinforced as part of a planned programme of assemblies*
- *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 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.*
- *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 / academy.*
- *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 students / 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, students 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 Technical Staff (or other relevant designated 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.*

Education – Parents / Carers

Parents play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. The school will seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, web site, Learning Platform*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications e.g. www.swgfl.org.uk*
- *www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers> (see*
- *appendix for further links / resources)*

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 each Autumn term.*
- *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.*

Technical – infrastructure / equipment, filtering and monitoring

Our SLA provides this through IT Services with CCBC. We also have support through device management from iTeach via SLA.

- Servers, wireless systems and cabling must be securely located and physical access restricted*
- All users will have clearly defined access rights to school technical systems and devices.*
- Where users need a password, the co-ordinator will create and share with classteachers. This information is stored on the school server*

Users are responsible for the security of their username and password

- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider.*
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.*

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupil's 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 online or 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 e.g. on social networking sites.*
- *Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press*
- *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 is not covered by the Data Protection Act).*
- *To respect everyone's privacy and in some cases protection, these images should not be published 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 / academy policies concerning the sharing, distribution and publication of those images.*
- *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.*

Data Protection - See policy for more detail

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

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- 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.
- 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 clear and understood arrangements for the security, storage and transfer of personal data
- 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 (many memory sticks / cards and other mobile devices cannot be password protected)
 - the device must offer approved virus and malware checking software the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

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.
- 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, Seesaw, VLE 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.
- 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

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. 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 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.

All staff working at any educational establishment are expected to demonstrate a professional approach and respect for pupils and their families and for colleagues and the learning setting.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to 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 students / 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.

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities eg cyber-bullying would be

banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions

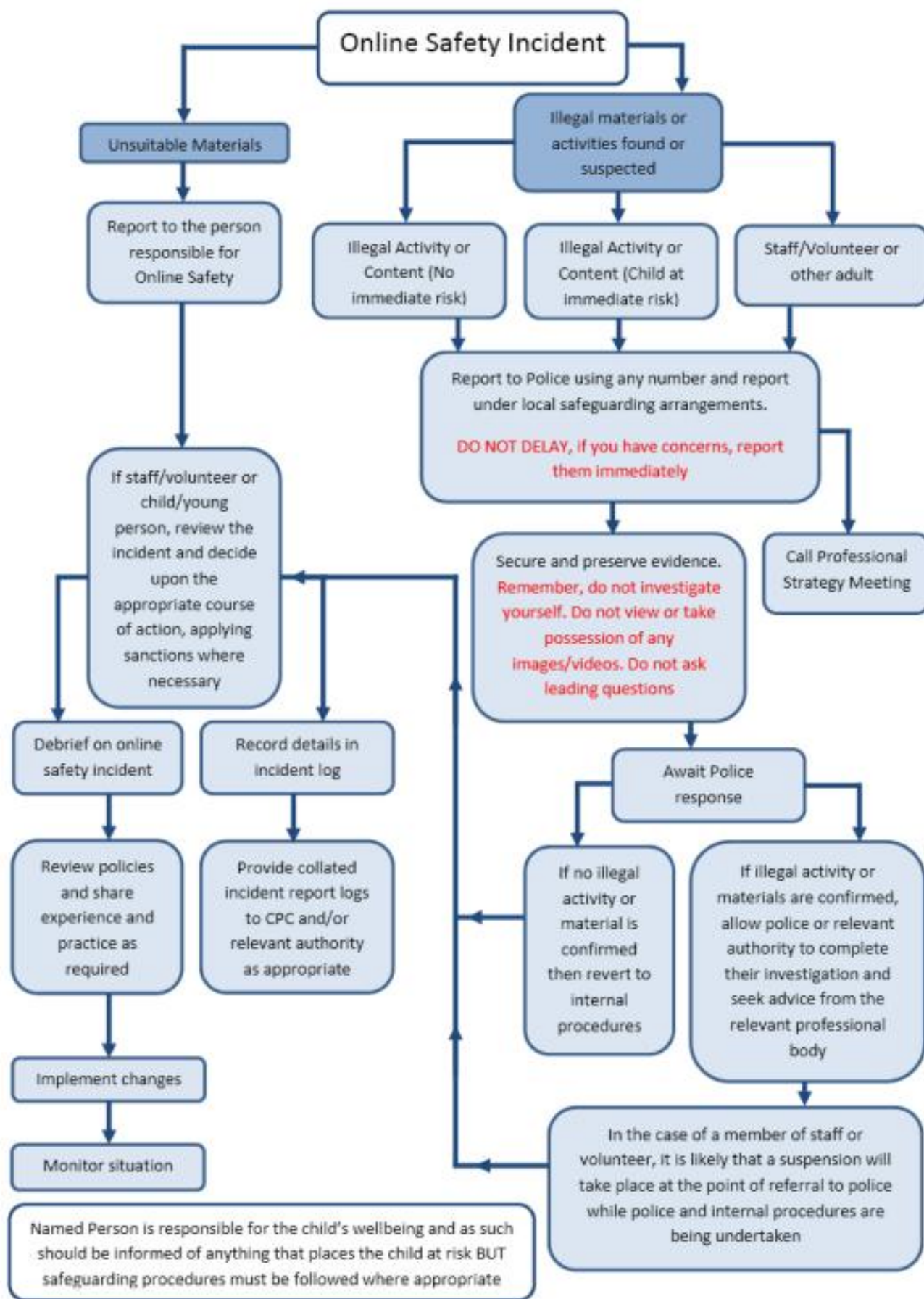
		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –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				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					

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 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 safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Online Bullying

If there is an allegation of online bullying , an incident recording form is opened to investigate. Both target and perpetrator and families are contacted. In some cases it necessary to report on to Police and/or Children's Services. The online form follows WG guidance from the Hwb Anti-bullying Strategy toolkit. This form is also available on our website.

Internet Safety Links

<https://www.parentsprotect.co.uk/internet-safety-links.htm>

<https://www.thinkuknow.co.uk/>

<https://anti-bullyingalliance.org.uk/>

<https://www.ceop.police.uk/Safety-Centre/>

Students / Pupils

Actions

[illegible]

Staff

Actions

Incidents:	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering	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								
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								

Online bullying incident recording form

Name of person reporting the incident:	
Name of staff member recording incident:	
Date of report:	

Type of online bullying incident (please tick all that apply):

Via mobile	☐	Persistent teasing/sarcasm	☐
Via gaming device	☐	Name-calling	☐
Via social media	☐	Threats	☐
Via chatroom	☐	Spreading rumours	☐
Via photographs	☐	Unpleasant/hurtful texts/messaging/web posts combined	☐
Via messaging apps	☐	Plans to isolate someone	☐
Misuse of image or video	☐	Ridicule/humiliation	☐

<i>Sexual</i>	☐	<i>Focused on family status or looked after child (LAC) status</i>	☐
<i>Focused on gender identity</i>	☐	<i>Focused on appearance</i>	☐
<i>Other (please state):</i>			

<i>Name of alleged target:</i>			
<i>Class/form/age</i>		<i>Year group/house</i>	

<i>Name of alleged perpetrator(s) if known</i>		1)	
2)		3)	
<i>Class/form/age</i>		<i>Year group/house</i>	

	<i>Day</i>	<i>Month</i>	<i>Year</i>
--	------------	--------------	-------------

<i>Date(s) of incident(s)</i>					
<i>Approximate time(s)</i>	<i>Before school</i>	<i>Morning</i>	<i>Afternoon</i>	<i>After school</i>	<i>Weekend</i>

Safeguarding considerations

If there is or might be a significant risk of harm, talk to your designated safeguarding lead in school (DSL).

The school has the powers to search and confiscate a phone. (EIA 2006). Have regard for protocols on safe handling of evidence or mobiles. Do not view, store or share material that contains intimate images of a learner without consulting the DSL.

Details

<i>How long has the bullying been going on?</i>

<i>Has any intervention been tried?</i>	Yes ☐	No ☐
---	------------------------------	-----------------------------

<i>If abusive, has the incident been reported to the service provider or website?</i>	Yes ☐	No ☐
---	------------------------------	-----------------------------

<i>Has the Child Exploitation Online Protection command (CEOP) report abuse button been used?</i>	Yes ☐	No ☐
---	------------------------------	-----------------------------

<i>Does this case require the serious incident protocol to be activated?</i>	Yes ☐	No ☐
--	------------------------------	-----------------------------

<i>Do the police need to be informed?</i>	Yes ☐	No ☐
---	------------------------------	-----------------------------

<i>Does a device or evidence need to be confiscated/isolated as evidence?</i>	Yes ☐	No ☐
---	------------------------------	-----------------------------

<i>Does material need to be taken down?</i>	Yes ☐	No ☐
---	------------------------------	-----------------------------

<i>Have parents/carers been informed?</i>	Yes ☐	No ☐
---	------------------------------	-----------------------------

Who has taken responsibility for these steps?

Follow-up

Has the online bullying stopped? Does the learner (target) feel safe?

Yes ☐

No ☐

Is further action required?

Yes ☐

No ☐

Have those involved changed their behaviour/acknowledged the harm caused?

Yes ☐

No ☐

Has the case contributed to the learning of the class/year group in some way?

Yes ☐

No ☐

Have passwords been changed, privacy settings checked and friends list cleaned?	Yes ☐	No ☐	N/A ☐
---	------------------------------	-----------------------------	------------------------------

If you have triggered the serious incident protocol, that will take precedence over anything in this document.

Any further notes, such as the impact of this incident or recommendations

Signed..... Date