

## e-Safety Policy March 2020

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

To be reviewed Spring Term 2023

Adopted by: \_\_\_\_\_ Date: \_\_\_\_\_

## Development / Monitoring / Review of this Policy

This e-Safety policy has been developed using a Welsh Government provided template and advice from the Local Authority by the Headteacher, Deputy Headteacher and members of the school council.

## Schedule for Development / Monitoring / Review

This e-Safety policy was approved by the Governing Body / Governors Sub Committee on:	
The implementation of this e-Safety policy will be monitored by the:	Headteacher and ICT Lead
Monitoring will take place at regular intervals:	Spring Term every three years
The Governing Body / Governors Sub Committee 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:	Any incidents will be reported as part of the Safeguarding Report in the termly report to Governors
The e-Safety Policy will be reviewed every three years or annually 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 2023
Should serious e-Safety incidents take place, the following external persons / agencies should be informed:	Local Authority Designated Officer and Mr. John Burge (School and Family Support Unit) Mrs. Sam Jones (LADO)

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Listening to Learners about ICT use
- Reports from LA regarding inappropriate Internet use

## Roles and Responsibilities

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 Governing body receiving regular information about e-Safety incidents and monitoring reports. A member of the Governing Body should take on the role of e-Safety Governor to include:

- regular meetings with the Headteacher/ICT Lead
- regular monitoring of e-Safety incident logs
- regular monitoring of filtering / change control logs

### Headteacher / Principal and Senior Leaders:

- **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 may be delegated to the ICT Lead.
- **The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management 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.**
- The Headteacher is responsible for ensuring that the e-Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.

### e-Safety Coordinator / Officer:

The e-Safety Coordinator / Officer is the Headteacher or, in their absence, the deputy headteacher

- 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 (or identifies sources of) training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with authority 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 if possible, filtering / change control logs
- reports regularly to Senior Leadership Team

### Network Manager / Technical staff:

NOTE: If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the e-Safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school e-Safety policy and procedures.

The Authority Technical Staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets (as a minimum) the required e-Safety technical requirements as identified by the Local Authority or other relevant body and also the e-Safety Policy / Guidance that may apply.

- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that the filtering policy (if one exists), is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- that they keep up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction
- that (if present) monitoring software / systems are implemented and updated as agreed in school policies

## **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 / AUA)
- they report any suspected misuse or problem to the Headteacher for investigation / action
- 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 agreements / 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 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

## **Safeguarding Designated Person**

The Safeguarding Designated Person 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

## **ICT/Science/PSD Group**

Members of the e-Safety Group will assist the Headteacher with:

- the production / review / monitoring of the school e-Safety policy / documents.
- 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 students / pupils about the e-Safety provision
- monitoring improvement actions identified through use of the 360 degree safe Cymru self review tool

## **Pupils:**

- **are responsible for using the school digital technology systems in accordance with the Student / 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. The school will take every opportunity to help parents understand these issues through 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 student / pupil records

## **Policy Statements**

### **Education – young people**

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of students 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 ICT and Digital Literacy lessons or other lessons and should be regularly revisited
- Key e-Safety messages should be reinforced as part of a planned programme of assemblies and 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.

## **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,
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg <https://hwb.wales.gov.uk/>  
[www.saferinternet.org.uk/](http://www.saferinternet.org.uk/) <http://www.childnet.com/parents-and-carers> on the school website

## **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 / Officer (or other nominated person) will receive regular updates through attendance at external training events (eg from Consortium / SWGfL / LA / other relevant organisations) 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 / team meetings / INSET days.
- The e-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

## **Training – Governors**

Governors should take part in e-Safety training / awareness sessions. 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**

The school will be 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. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-Safety responsibilities:

- 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 must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All staff users will be provided with a username and secure password by the ICT Lead who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every term

- All pupils users will use the 'group log in' system to sign onto the machines to access the internet. Pupils will have individual HWB log ins from that point to access the VLE.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher / Principal or other nominated senior leader and kept in a secure place (eg school safe)
- The school Bursar 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
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes through the Headteacher
- The school has provided enhanced / differentiated user-level filtering allowing different filtering levels for different groups of users – staff / pupils / headteacher)
- An appropriate system is in place where staff report any actual / potential technical incident / security breach to the Headteacher, Deputy Headteacher or ICT Lead.
- 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" (eg trainee teachers, supply teachers, visitors) onto the school systems through the 'Bring Your Own Device' network which is password controlled.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- Staff and pupils may not download executable files and installing programmes on school devices.
- Removable media (eg memory sticks / CDs / DVDs) are not to be used 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 on the HWB portal.

## 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 students / 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 is 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 students / 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, blog or feed, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

## Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Data Protection Act 2018 and subsequent GDPR 2018 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". (see Privacy Notice section in the appendix)
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

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

When personal data is stored on any portable computer system:

- the data must be encrypted and password protected
- the device must 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
- remember that portable media and storage devices are not permitted to be used.



# 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:

Communication Technologies	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Not allowed	Allowed	Allowed at certain times owed 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 school tablets,								
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 students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (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 students / pupils or parents / carers (email, chat, 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.
- Whole class / group email addresses may be used at Foundation Phase, while pupils at KS2 and above will be provided with individual school email addresses for educational use through HWB.
- 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' and Teaching Assistants' professional conduct are set out by the Education Workforce Council (ECW) 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.

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.

## Unsuitable / inappropriate activities

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 users	Unacceptable	Unacceptable and illegal
<b>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:</b>	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)		X				
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce		X				
File sharing					X	

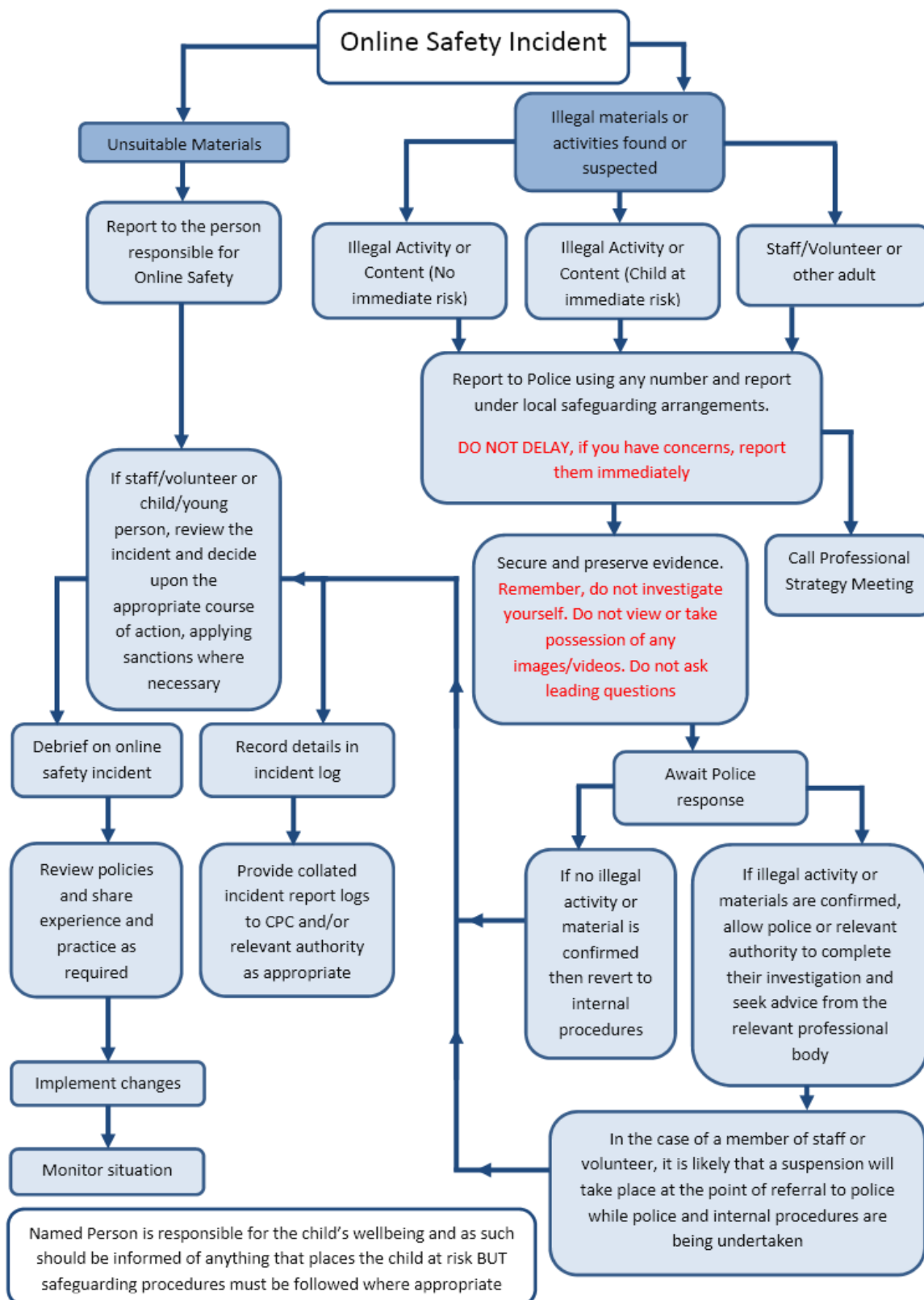
Use of social media				X	
Use of messaging apps				X	
Use of video broadcasting eg Youtube				X	

## 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 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 within the school as agreed by the Governing Body.

Incidents:	Refer to class teacher / tutor	Refer to Headteacher / Principal	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
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>		X	X					
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device		X			X			X
Unauthorised use of social media / messaging apps / personal email		X			X			X
Unauthorised downloading or uploading of files		X			X	X		X
Allowing others to access school network by sharing username and passwords	X						X	
Attempting to access or accessing the school network, using another student's / pupil's 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
Corrupting or destroying the data of other users		X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X	X		X
Continued infringements of the above, following previous warnings or sanctions		X	X		X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		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	
Deliberately accessing or trying to access offensive or pornographic material		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		

## 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 etc	Warning	Suspension	Disciplinary action
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>		X	X	X				
Inappropriate personal use of the internet / social media / personal email		X	X			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 or attempting to access or accessing the school network, using another person's account		X	X		X	X	X	X
Careless use of personal data eg holding or transferring data in an insecure manner		X	X				X	
Deliberate actions to breach data protection or network security rules		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 email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X	X		X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X		X		X	X
Actions which could compromise the staff member's professional standing		X	X			X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X			X	X	X
Using proxy sites or other means to subvert the school's filtering system		X	X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X			X		
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X	X	X
Breaching copyright or licensing regulations		X	X		X	X		
Continued infringements of the above, following previous warnings or sanctions		X	X		X	X	X	X



## **Appendices – Section A - Acceptable Use Agreement**

• A1 Student / Pupil Acceptable Use Agreement template (younger children)	18
• A2 Student / Pupil Acceptable Use Agreement template (older children)	19
• A3 Staff and Volunteers Acceptable Use Agreement template	21
• A4 Parents / Carers Acceptable Use Agreement template	24
• A5 Community Users Acceptable Use Agreement template	26

## **Appendices – Section C – Support documents and links**

• C1 Responding to incidents of misuse – flowchart	27
• C2 Record of reviewing sites (for internet misuse)	28
• C3 School Reporting Log template	29
• C4 School Training Needs Audit template	30

**A1: Acceptable Use document for use of School Equipment and Hwb+**

Hwb+ is a cool school tool!

- Be polite - don't upset or bully anyone.
- If you feel upset or bullied, tell a teacher right away. Use the Worry Box if you want.



Worry Box

- Be safe – don't tell anyone where you live or what your phone number is.
- Be security smart - keep your username and password safe.
- Only send and open emails if told to by your teacher. If you are unsure, always check with your teacher first.
- I understand that all of my work can be seen by my teacher.

**I understand that I must follow these rules or I might be in trouble. However, if it's not your fault you won't be in trouble.**



I agree with what I have read above and/or what my teachers have told me about using Hwb+ properly.

Name of child: NAME OF CHILD Date: DD / MM / YY

Signature: SIGNATURE Class: Class name

## **A2: Key Stage Two Acceptable Use agreement for School Equipment and Hwb+**

Hwb+ is a cool, school tool!

Remember, anything you do on Hwb+ should have an educational purpose.

- Be polite - don't upset or bully anyone.
- Be polite - never post something online on Hwb+ or send an email which is likely to cause offence to someone else. Don't upset or bully anyone.
- Be polite - never post something online in Hwb+ or send an email which is likely to cause offence to someone else. Leave a positive impression of yourself online. You never know, your future college, University, or employer may look at your online life.
  
- Be safe – don't tell anyone where you live or what your phone number is
- Be safe – don't reveal anything about yourself or about your friends (especially home address or phone numbers). This is very important.
- Be safe – don't reveal anything about yourself or about your friends, especially personal addresses or other contact details.
  
- If you feel upset or bullied, tell a teacher right away. Use the Worry Box if you want.
- Protect the school community by telling a teacher if you see anything that might cause upset or harm to yourself, other pupils or teachers in the school. Use the Worry Box if you want.
- Protect the school community by reporting to a teacher anything you see that might cause upset or harm to yourself, other pupils or teachers in the school.
  
- Be careful what you say and how you say it. What you do and say on Hwb+ is recorded and will be viewed by other people including your teacher.
- Use appropriate language at all times and within an educational theme. What you say on Hwb+ is recorded and will be viewed by other people including your teachers.
  
- Be security smart - keep your username and password safe.
- Be security smart - keep your username and password safe. Someone might get on to your Hwb+ account if you don't and can read all of your emails.
- Be security smart - keep your username and password safe. You are responsible for anything that happens under your Hwb+ account.
  
- Only link to other websites if you are sure they are safe to visit and are appropriate for your classmates and friends.

- If you share website links within Hwb+, then you agree that the content of the external website is appropriate and has an educational purpose.
- Only send and open emails if told to by your teacher. If you are unsure, always check with your teacher first.
- Send emails as directed by your teacher – don't communicate with people you or your teachers don't know. Don't open emails if you don't know the sender. If you are unsure, always check with your teacher. Email use may be monitored.
- Don't communicate (share documents or email) with people you don't know unless directed by your teacher. Email use may be monitored. Don't put anything in your skydrive/e-portfolio that you can't share with your teacher.
- I understand that all of my work can be seen by my teacher.
- Don't upload anything to the platform that you can't share with your teacher.
- Content relating to or supporting illegal activities may be reported to the authorities.
- Always keep another local copy of your essential work that you store on skydrive
- I understand that I must follow these rules or I might be in trouble. However, if it's not your fault you won't be in trouble.
- Your school may have to look at taking you offline if you cannot accept these rules which are for the good of everyone, yourself included.
- Unacceptable use within Hwb+ (as highlighted but not limited to that above) might result in actions taken in line with the school's Disciplinary Policy.
- I agree with what I have read above and/or what my teachers have told me about using Hwb+ properly.
- I do/do not agree with the Acceptable Use statements above.
- I do/do not agree to the Terms of Use as outlined above.

Signed: \_\_\_\_\_ (pupil)

Signed: \_\_\_\_\_ (parent)

Date: \_\_\_\_\_

# **A3 Staff (and Volunteer) Acceptable Use Policy Agreement Form**

## **School Policy**

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

### **This Acceptable Use Policy is intended to ensure:**

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

## **Acceptable Use Policy Agreement**

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-Safety in my work with young people.

### **For my professional and personal safety:**

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not use my mobile phone in school lesson time, unless in case of emergency or without the prior consent of the Headteacher

### **I will be professional in my communications and actions when using school ICT systems:**

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies. (schools should amend this section to take account of their policy on access to social networking and similar sites)
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with students / pupils and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)
- I will not engage in any on-line activity that may compromise my professional responsibilities.

**The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school :**

- When I use my mobile devices (PDAs / laptops / mobile phones) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. I will not use a removable storage device in school or store school information on it.
- I will not use personal email addresses on the school ICT systems unless for work related purposes.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

**When using the internet in my professional capacity or for school sanctioned personal use:**

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

**I understand that I am responsible for my actions in and out of the school:**

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

## A4 Parent / Carer Acceptable Use Agreement Form

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

### This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Agreement is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

### Permission Form

Parent / Carers Name

Pupil Name

As the parent / carer of the above pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

#### Key Stage Two (Juniors)

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

#### Foundation Phase (Infants)

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, e-Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including applying monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-Safety.

Signed

Date



## Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use school digital cameras or iPads to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people can not be identified by the use of their names.

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 / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree.

### Digital / Video Images Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above student / pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

Yes / No

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Yes / No

Signed

Date

## A5 Acceptable Use Agreement for Community Users Template

### This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices.
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices.

### Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

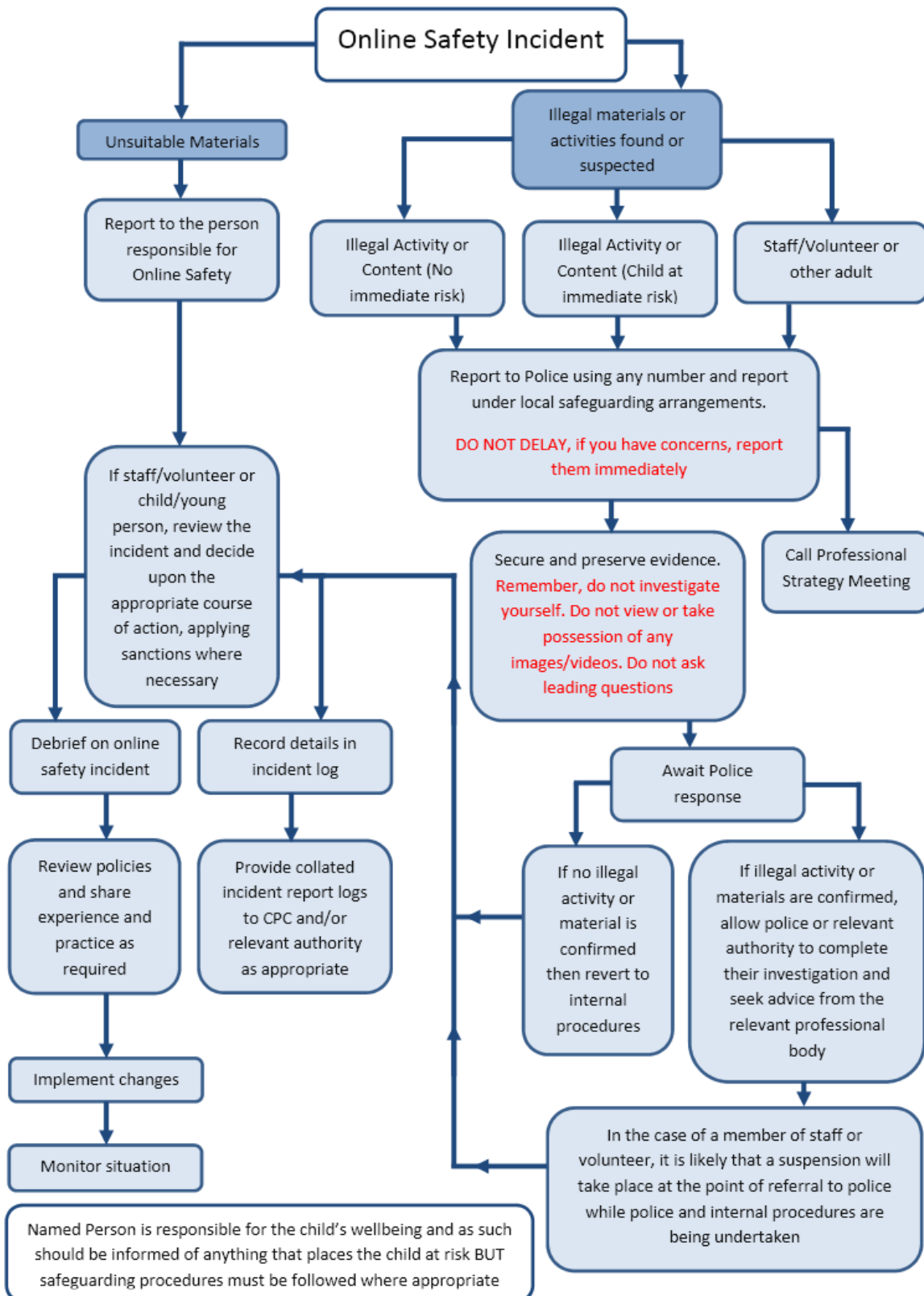
I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name

Signed

Date

## C1 Responding to incidents of misuse – flow chart



**C2 Record of reviewing devices / internet sites (responding to incidents of misuse)**

Group	
Date	
Reason for investigation	

**Details of first reviewing person**

Name	
Position	
Signature	

**Details of second reviewing person**

Name	
Position	
Signature	

**Name and location of computer used for review (for web sites)**

--

**Web site(s) address / device**

**Reason for concern**


**Conclusion and Action proposed or taken**


### C3 Template Reporting Log

Reporting Log Group .....							Signature
Date	Time	Incident	Action taken		Incident Reported by		
			What?	By whom?			

## C4 Training Needs Audit

Training Needs Audit Log							
Group .....	Date .....						
Name	Position	Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date	