E-Safety Policy

This e-safety policy was approved by the *Governing Body / Governors Sub Committee on:*	*6th November 2018*
The implementation of this e-safety policy will be monitored by the:	*E-Safety Coordinator*
Monitoring will take place at regular intervals:	*Annually*
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:	*Annually*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*Annually*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA Schools ICT Strategic Manager, LA Safeguarding Officer, Police Commissioner's Office*

Schedule for Development / Monitoring / Review

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity (school that manage their own filtering)*
- *Surveys / questionnaires of*
  - *students / pupils (eg CEOP ThinkUknow survey)*
  - parents / carers
  - staff

Background / Rationale

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

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

Some of the potential risks could include:

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

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

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

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

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a Strategic e-Safety working group made up of Headteachers, High School and Primary School ICT Leaders and Local Authority Staff and has been reviewed by a wide range of relevant stakeholders.

Consultation with the whole school community has taken place through a variety of informal and formal meetings:

Scope of the Policy

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 school.

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

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

Roles and Responsibilities

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

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 *Governors / Governors Sub Committee* receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of *E-Safety Governor.* The role of the E-Safety Governor will include:

- *regular meetings with the E-Safety Co-ordinator / Officer*
- *regular monitoring of e-safety incident logs*
- *regular monitoring of filtering / change control logs*
- *reporting to relevant Governors committee / meeting*

Headteacher and Senior Leaders:

- **The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community**, though the day to day responsibility for e-safety will be delegated to the *E-Safety Co-ordinator / Officer (see below)*.
- *The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant*
- *The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
- *The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the E-Safety Co-ordinator / Officer.*
- **The Headteacher and 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.** (see flow chart on dealing with e-safety incidents and online safety incident included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)

E-Safety Coordinator / Officer: Ms Sofianos

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff including how to be alert to the potential misuse of digital media and take responsibility for reporting it appropriately
- liaises with the Local Authority
- liaises with ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments (see appendix).
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

Please see Appendix One.

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 school Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the E-Safety Co-ordinator / Officer /Headteacher / Senior Leader / Head of ICT / ICT Co-ordinator / Class teacher / Head of Year (as in the section above) for investigation / action / sanction**
- **all digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) 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 school activities
- students / pupils understand and follow the school e-safety and acceptable use policy
- 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 lesson 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*

Designated person for child protection / Child Protection Officer : Mrs J Thomas / Mr M Harries

should be trained in e-safety issues and be aware of the potential for serious child protection 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

E-Safety Committee

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

Members of the *E-safety Group* (or other relevant group) will assist the *E-Safety Coordinator / Officer (or other relevant person, as above)* with:

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

- *the production / review / monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.*
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool

Students / pupils:

- **are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of safe use of digital media and how to report abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website / VLE 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
- their children's personal devices in the school / academy (where this is allowed)
- digital media and how to report abuse, misuse or access to inappropriate materials

Visiting Adults and Pupils

Users who access school ICT systems / website / VLE via login as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

Policy Statements

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students / 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 Computing / PHSE / other lessons and should be regularly revisited**
- **Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities**
- **Students / 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.**
- **Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- *Students / pupils should be helped to understand the need for the student / 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 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 students / 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.*
- *Students should be supported to understand and report unsafe or harmful digital misuse.*

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: (select / delete as appropriate)

- *Curriculum activities*
- *Letters, newsletters, web site, VLE*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns eg Safer Internet Day*
- *Reference to the relevant web sites / publications eg www.swgfl.org.uk* www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

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

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

Cyberbullying

Cyber bullying has become an increasing concern for schools, parents and children alike. Cyber bullying has traditionally been defined as harassment and victimisation using interactive technology. It is important that we understand the complex nature of cyber bullying to be able to prevent incidents and respond effectively to incidents when they arise. For example, one comment made online becomes bullying when it is repeatedly forwarded or commented on by others, which in turn is seen by multiple people over a sustained period of time. It can often be difficult to gain closure when subject to a cyber-bullying incident when the comment or photo can resurface at any time.

Cyber bullying differs from traditional forms of bullying and can have a significant detrimental impact upon individuals who are targeted by such behaviour. The 24/7 nature of cyber bullying can make it difficult for a target to escape the attacks directed at them. In some cases an individual may not know they are being bullied if they have not seen the content posted about them, but it is important to understand that the intentions of the perpetrator is still to bully the individual in question by posting humiliating and hurtful content.

We promote the positive use of Interactive Technology and Social Media, where pupils are provided with opportunities to discover the benefits social media has to their learning and social development. We understand that it can sometimes be easy to forget that we are talking to real people with real emotions when using social media; as such we encourage and promote responsible use and respectful communications with others online.

All incidents of inappropriate use of social media are taken seriously and we encourage all members of the school community to report any incidents of inappropriate use of social media and interactive technology.

Inappropriate use of social media includes, but not restricted too:

- harassment and intimidation of others,
- sending hateful messages,
- posting inappropriate and unwanted pictures online and;

- creating content which has the potential to hurt, embarrass and humiliate others.
- Sexting
- Online exploitation including sexual abuse

We respond to inappropriate use and bullying online in accordance with the procedures and guidance outlined in our anti-bullying and behaviour policy. Support is provided to all parties involved in incidents of bullying online and parents will be notified following a report of bullying online. Where appropriate we will contact external agencies to obtain further advice, information and provide additional support to individuals if necessary. Restorative approaches will be implemented to resolve any issues of inappropriate use of social media. We understand that in some circumstances there will be a requirement to involve the police. We will liaise with our Police School Liaison Officer for advice on the appropriate route and action to take in these circumstances.

Education & Training – Staff

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. 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 Policies**
- *The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at Consortium/ LA / other information / training sessions and by reviewing guidance documents released by BECTA / Consortium / LA and others.*
- *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 (or other nominated person) will provide advice / guidance / training as required to individuals as required*

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

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

Technical – infrastructure / equipment, filtering and monitoring

Please see Appendix One.

Bring your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's / academy's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students / Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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 students / 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.**
- *Staff 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.***
- *Schools are advised to ensure that policies on the storage and destruction of images are in place*
- *Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- *Students / 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.*
- *Students' / Pupils' full names will not be used in association with photograph, unless enhanced signed consent has been given.*
- *Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year* (see Parents / Carers AUP Agreement in the appendix)
- *Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.*

Data Protection

For staff members, please refer to corporate Acceptable Use Policies, Data Protection Policies and school data protection policies.

Communications

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

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times / places	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times / places	Allowed with staff permission	Not allowed
Mobile phones may be brought to school		√						√
Use of mobile phones in lessons				√				√
Use of mobile phones in social time	√							√
Taking photos on personal mobile phones or other camera devices				√				√
Use of other mobile devices eg tablets, gaming devices				√				√
Use of personal email addresses in school, or on school network		√					√	
Use of school email for personal emails				√				√
Use of chat rooms / facilities			√					√
Use of instant messaging/messaging apps			√					√
Use of social networking sites			√					√
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.** *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 need to be aware that email communications may be monitored**
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.**
- **Any digital communication concerning school (email, chat, VLE etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems.*
- *The use of personal email addresses, text messaging or public chat / social networking programmes **must not be used** for professional purposes. Staff should remain professional in tone and content when discussing school online and should not bring the school into disrepute.*
- *Whole class or group email addresses will be used at FP, while students / pupils at KS2 and above can be provided with individual school email addresses for educational use.*
- *Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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 / academy					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

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

The flow chart on the next page should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

Social Media – Protecting Professional Identity

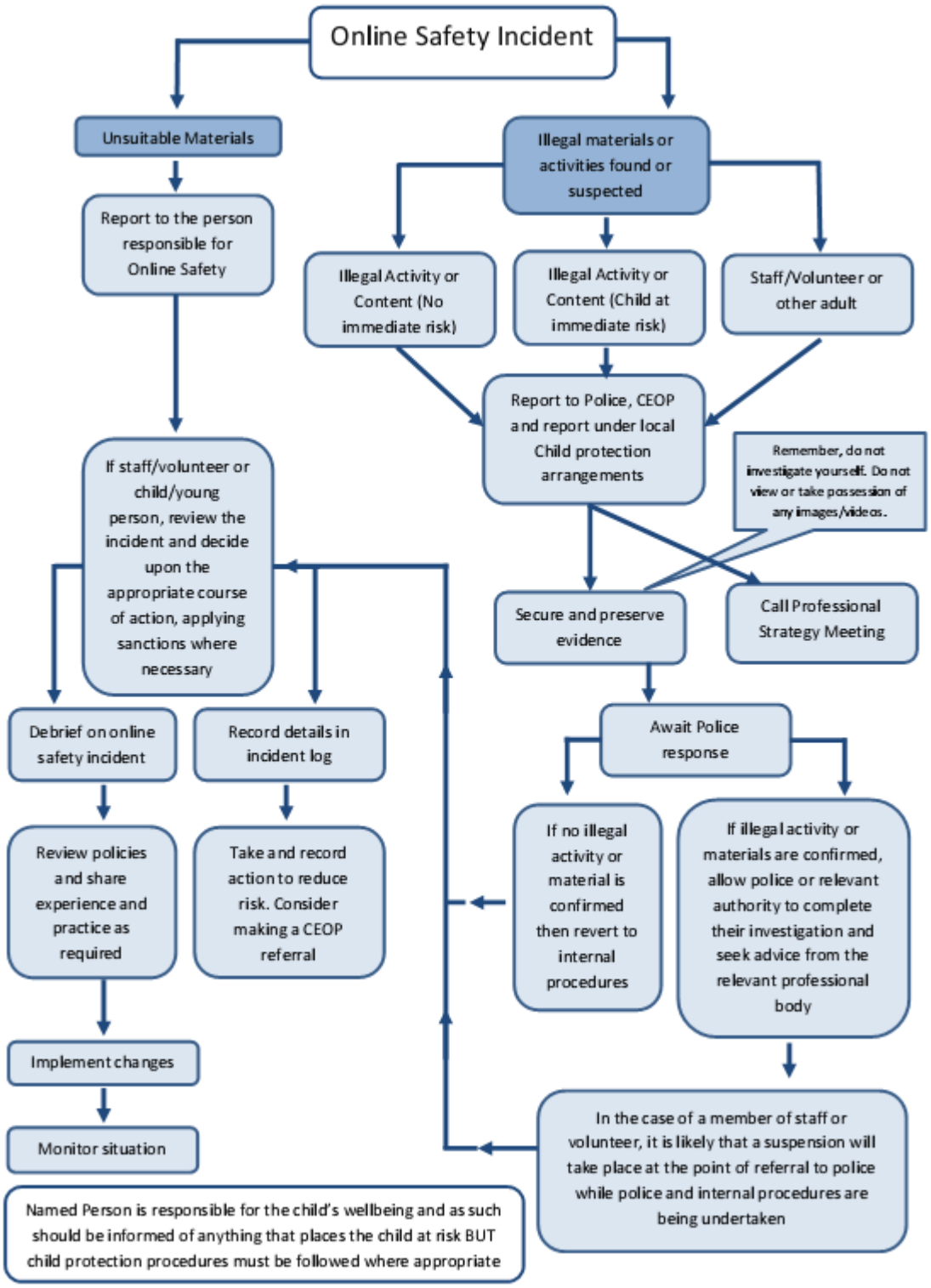
All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

- The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:
- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to 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.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review policies and share experience and practice as required
Take and record action to reduce risk. Consider making a CEOP referral
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk BUT child protection procedures must be followed where appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at immediate risk)
Staff/Volunteer or other adult
Report to Police, CEOP and report under local Child protection arrangements
Remember, do not investigate yourself. Do not view or take possession of any images/videos.
Secure and preserve evidence
Call Professional Strategy Meeting
Await Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police while police and internal procedures are being undertaken

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the “Guidance for Reviewing Internet Sites for Suspected Harassment and Distress “should be followed. This can be found in the appendix. This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a “clean and designated” computer.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:

Students / Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓	✓			
Unauthorised use of non-educational sites during lessons		√							
Unauthorised use of mobile phone / digital camera / other handheld device			√						
Unauthorised use of social networking / messaging apps / personal email			√						
Unauthorised downloading or uploading of files			√						
Allowing others to access school network by sharing username and passwords			√						
Attempting to access or accessing the school network, using another student’s / pupil’s account			√						

Attempting to access or accessing the school network, using the account of a member of staff			√						
Corrupting or destroying the data of other users			√						
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			√			√			
Continued infringements of the above, following previous warnings or sanctions			√			√			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			√			√			
Using proxy sites or other means to subvert the school'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			√			√			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			√			√			

Actions / Sanctions

Staff

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓			
Inappropriate personal use of the internet / social networking sites / instant messaging / 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 instant 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		√	√					
Continued infringements of the above, following previous warnings or sanctions		√				√		

Acknowledgements

Merthyr Tydfil County Borough Council would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School E-Safety Policy Template:

- SWGFL for their processes, procedures and work to initially create the sample policy that this is based on.
- CSC JES
- All internal and external reviewers and stakeholders
- Consortium Colleagues in Rhondda Cynon Taf, Cardiff, Neath Port Talbot, Bridgend and The Vale of Glamorgan for reviewing and approving this document.
- Merthyr Tydfil Schools ICT Strategic Group e-Safety working group.
- Cardiff Council Schools e-Safety sub-committee
- Merthyr Tydfil Corporate IT Department and Information Security Officer

Date on which policy was approved by Governing Body: 2018/2019

Policy review date: Annually

Appendix One

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

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

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

Context

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

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

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

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

- Standards of security and controls implemented will need to be equivalent to those outlined in this and other supporting policy documents.

- The security of the schools' Shared Network should not be jeopardised or undermined

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

Connections to the Schools' Network

- Equipment connected to the Shared Schools Network should be owned by the school and in line with the limitations set out in the Schools ICT Support SLA

- Antivirus: In line with the Schools Broadband Terms and Conditions, it is the school's responsibility to ensure workstations and other devices are protected by up to date virus software.

- Appropriate security measures are in place to protect the servers, networking equipment, work stations, hand held devices, etc from accidental or malicious attempts which might threaten the security of the school systems and data. These measures should not be circumvented or attempts made to do so.

Internet Filtering

- The school uses and supports the managed filtering service provided by MTCBC ICT Department
- Any filtering issues should be reported immediately to the MTCBC ICT Department (Schools ICT) Helpdesk.
- The School's own Internet Acceptable Use Policy uses the whole of the MTCBC ICT Internet Policy as a baseline – adding policy statements applicable to the local context if needed.
- In accordance with the MTCBC Internet Acceptable Use Policy, school ICT technical or MTCBC ICT staff may monitor and record the activity of users on the school ICT systems. Users are made aware of this in the Acceptable Use Policy.

Access, Controls and Restrictions

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

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

Information Security

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

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