E-Safety Policy

SUCCESS, TOGETHER, ASPIRE, RESPECT

Policy development:

Document name:	E-Safety	
Date of issue:	02/09/2021	
Governor ratification:	Awaiting Governor Ratification	

Version control:

Date:	**Version:**	**Updates/changes:**
02/09/2021	3	02/09/2021

Table of Contents

1. Schedule for Development / Monitoring / Review

This E-Safety policy was approved by the Governing Body on:	1/09/20 (Next Review Oct 2021)
The implementation of this E-Safety policy will be monitored by the:	Designated Safeguarding Lead, Senior Leadership Team, Network Manager/IT Technicians
Monitoring will take place at regular intervals:	Annually – or following statutory changes
The Governing Body via the appropriate 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).	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:	September 2022
Should serious E-Safety incidents take place, the following external persons / agencies should be informed:	LADO, MASH Team, LA Safeguarding Officer, Police.
Local Authority Lead Safeguarding Officer for Education	Gina Andrews 0161 253 5811/ 07974 604 223 g.andrews@bury.gov.uk

2. Scope of the Policy

This policy applies to all members of the School Community (including Staff, Pupils, Volunteers,) who have access to and are users of School's ICT systems, both in and out of the School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the 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 outside of the School, but is linked to membership of the School.

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 take place out of School.

3. Roles and Responsibilities

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the School:

3.1 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 relevant Governors' Sub Committee receiving information via the DSL SLT reporting Data from My Concern. A member of the Governing Body has taken on the role of E-Safety Link Governor. The role of the E-Safety Governor will include:

- meetings with the DSL (Designated Safeguarding Lead)
- reporting to relevant Governors' meetings

3.2 Headteacher 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 will be delegated to the DSL (Designated Safeguarding Lead) and DDSLs (Deputy Designated Safeguarding Leads).
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of Staff (Teaching or Non-Teaching). *See flow chart on dealing with E-Safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures.*
- The Headteacher / Senior Leaders are responsible for ensuring that the DSL (Designated Safeguarding Lead) and DDSLs (Deputy Designated Safeguarding Leads) and other relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in School who carry out these important internal E-Safety monitoring roles, thus providing a supportive safety net.

3.3 DSL (Designated Safeguarding Lead) and DDSLs (Deputy Designated Safeguarding Leads):

- take day to day responsibility for E-Safety issues, having a leading role in establishing and reviewing the School's E-Safety policies / documents.
- ensure that all Staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- provide training and advice for Staff
- liaise with the Local Authority / relevant body
- liaise with the School's IT Network Manager and Staff
- receive reports of E-Safety incidents (via Smoothwall) and record on MyConcern
- meet with E-Safety Link Governor to discuss current issues
- report when necessary to the Senior Leadership Team on any E-Safety matter.

Are trained in E-Safety issues and are aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- threat of terrorism or supporting terrorism
- inappropriate on-line contact with adults / strangers

- potential or actual incidents of grooming
- Cyber-Bullying

3.4 Network Manager:

The Network Manager is responsible for ensuring:

- that the School's technical infrastructure is secure and is not open to misuse or malicious attack
- that the School meets required E-Safety technical requirements and any Local Authority / other relevant body 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 Staff passwords are regularly changed
- the Filtering Policy is applied and updated on a regular basis
- that they keep up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform/ update others as relevant
- that the use of the network / internet / remote access is regularly monitored in order that any misuse / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / DSL (Designated Safeguarding Lead) and DDSLs (Deputy Designated Safeguarding Leads) for investigation / action / sanction

3.5 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
- they report any suspected misuse or problem to the Headteacher / DSL (Designated Safeguarding Lead) and DDSLs (Deputy Designated Safeguarding Leads) for investigation / action / sanction
- all digital communications with Pupils / Parents / Carers should be on a professional level and only carried out using official School systems
- E-Safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the E-Safety and Acceptable Use policies
- Pupils have a good understanding of research skills, the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other School activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

3.6 Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills, 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 's E-Safety Policy also covers their actions out of school, if related to their membership of the School.

3.7 Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The School will take every opportunity to help Parents understand these issues through Parents' Evenings, Newsletters, letters and school website. 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 / SIMS
- their children's personal devices in the School (where this is allowed)

4. Policy Statements

4.1 Education – Pupils:

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

E-Safety is a focus in key areas of the curriculum and Staff reinforce E-Safety messages across the curriculum. The E-Safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned E-Safety curriculum is provided as part of Computing and PHSE and is regularly revisited
- Key E-Safety messages are reinforced as part of a programme of Assemblies and Form Time activities
- Pupils are taught that when they are using computers they should be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside School
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that Pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where Pupils are allowed to freely search the internet, Staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, Staff can request that the Technical Staff 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.

4.2 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, especially in the monitoring / regulation of their children's on-line behaviours. Parents/ Carers may underestimate how often children and young people come across potentially harmful (and inappropriate) material on the internet. They 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, school twitter, text messages and latest information on the pastoral care section of the school website
- Parents / Carers evenings / Training sessions

4.3 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:

- All new Staff should receive E-Safety training as part of their *Induction* programme, ensuring that they fully understand the School's E-Safety Policy and Acceptable Use Agreements.
- DSL (Designated Safeguarding Lead) and DDSLs (Deputy Designated Safeguarding Leads) and Network Manager will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- DSL (Designated Safeguarding Lead) and DDSLs (Deputy Designated Safeguarding Leads) and Network Manager will provide advice / guidance / training to individuals/staff as required.

4.4 Training – Governors:

Governors should take part in E-Safety Training / Awareness sessions, with particular importance for those who are members of any Sub-Committee / group involved in Technology / 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 / or other relevant organisation.
- Participation in School Training / Information sessions for Staff or Parents.

5 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
- 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 users will be provided with a username and secure password. Users are responsible for the security of their username and password
- The Network Manager is responsible for ensuring that software licence logs are accurate, 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 is filtered by the broadband provider and by Philips High School using Smoothwall (Web Filtering Software). Smoothwall sends real time email notifications for any content which is categorised as inappropriate to the DSL (Designated Safeguarding Lead) and DDSLs (Deputy Designated Safeguarding Leads). The following categories are used to generate emails and monitoring reports: Adult Content, Bullying, Criminal Activity, Radicalisation, Abuse, Substance Abuse and Suicide.
- The DSL and DDSLs follow the 'Responding to incidents of misuse' flow chart in this document when they receive instant notification emails and monitoring reports.
    - Content lists are regularly updated by Smoothwall and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. Smoothwall is a member of the *Internet Watch Foundation (IWF)* and implement the CAIC List of domains and URLS. Smoothwall also use search terms and phrases provided by the IWF (and their members) in order to block websites and trigger email notifications.
- The School has provided enhanced / differentiated user-level filtering
- 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's systems and data. These are tested regularly. The School's infrastructure and individual workstations are protected by up to date virus software.
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the School's systems.
- School devices must not be used by anyone, including family members, unless they are employed by Philips High School.
- An agreed procedure is in place that allows Staff to / forbids Staff from downloading executable files and installing programmes on the School's devices.
- An agreed procedure is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on School devices. Personal data should not be taken off the School site unless safely encrypted or otherwise secured.

5.1 Use of Digital and Video Images:

The development of digital imaging technologies has created significant benefits to learning, allowing Staff and Pupils instant use of images that they have recorded themselves or downloaded from the internet. However, Staff, Parents / Carers and Pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for Cyber-Bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The School will inform and educate users about these risks in addition to implementing policies to reduce the likelihood of the potential for harm:

- When using digital images, Staff should inform and educate Pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet *e.g. on social networking sites*.
- Parents / Carers are not allowed to take videos and digital images of their children at School events for their own personal use. To respect everyone's privacy and in some cases protection, any images/videos provided by School 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 Safeguarding Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on School equipment; the personal equipment of Staff should not be used for such purposes.
- Care should be taken when taking digital / video images that Pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include Pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from Parents or Carers is obtained when pupils join the School; before photographs of Pupils are published on the School's website or any other published document. Permissions can be found on each Pupils SIMS profile.
- Pupil's work can only be published with the permission of the Pupil or Parent/Carer.

5.2 Communications:

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

	Staff & other adults				Pupils				
Communication Technologies	Not allowed	Allowed	Allowed at certain times	Allowed for educational purposes	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission for Educational purposes ONLY	N/A
Use of personal mobile phones with pupils present	X							X	
Use of mobile phones in social time		X					X		
Taking photos on personal mobile phones with pupils present	X				X				
Taking photos on school camera		X				X			
Use of other mobile devices e.g. tablets			X					X	
Use of personal email addresses in School, or on School network			X					X	
Use of School email for personal emails	X				X				
Use of messaging apps			X		X				
Use of social media			X		X				
Use of blogs				X				X	

When using communication technologies, the School considers the following as good practice:

- The official School email service may be regarded as safe and secure. Staff and Pupils should therefore use only the School email service to communicate with others when in School, or on the School's systems (e.g. by remote access).

- Users must immediately report, in accordance with the School Safeguarding Policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and ***must not respond to any such communication***.

- Any digital communication between Staff and Pupils or Parents / Carers (i.e. email) must be professional in tone and content. These communications may only take place on official School systems. ***Personal email addresses, text messaging or social media must not be used for these communications.***

- Pupils will be provided with individual School email addresses for educational use.

- Pupils will be taught about E-Safety issues, such as the risks attached to the sharing of personal details. They will 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's website and only official email addresses should be used to identify members of Staff.

5.3 Social Media - Protecting Professional Identity:

All Schools, Academies and Local Authorities (LA's) have a duty of care to provide a safe learning environment for Pupils and Staff. Schools and LA's 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 LA liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to Pupils, Parents / Carers or School Staff
- They do not engage in online discussion on personal matters relating to members of the School Community
- Personal opinions should not be attributed to the School or LA.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

For more information on *Social Media usage*, please see the ***Social Media Policy*** regarding professional conduct.

5.4 Unsuitable / inappropriate activities:

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

User 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
	Prevent – Using the School's system to become a terrorist or support terrorism.					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 (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
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 e.g. YouTube				X		

6. 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).

6.1 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 (Responding to Incidents of Misuse – Page 16) for responding to online safety incidents and report immediately to the police.

6.2 Other Incidents:

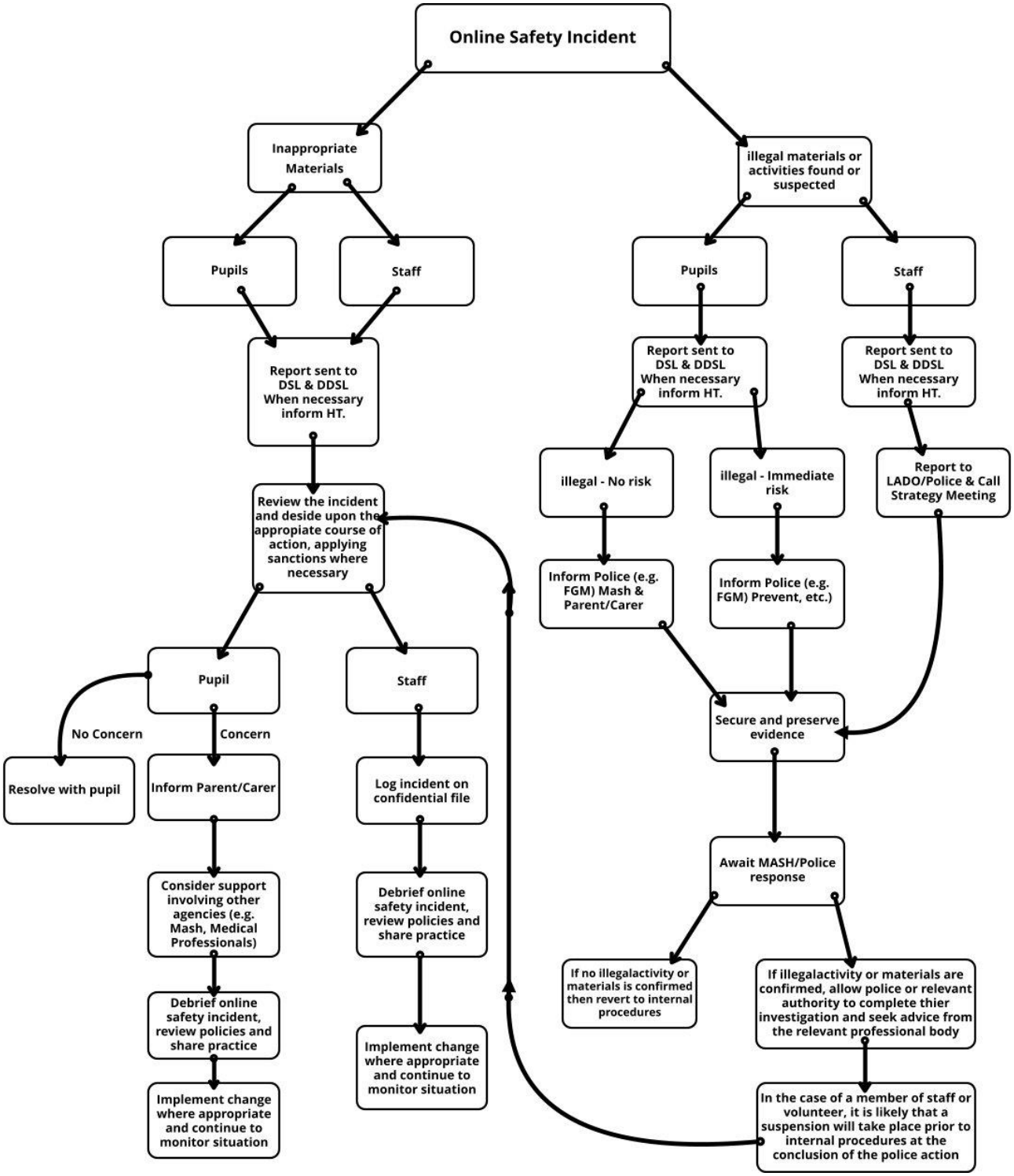
It is hoped that all members of the School community will be responsible users of digital technologies, who understand and follow School policy. However, there may be times when infringements of the policy could take place, through either carelessness, irresponsibility or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one *Senior* member of Staff 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 urn 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
- Using the School's system to become a terrorist or support terrorism.
- Potential case of FGM and other honour based violence.
- Other criminal conduct or potential 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.

6.3. Responding to Incidents of Misuse – Flow Chart

Any Online Safety Incidents must be recorded on My Concern.



6.4. School Actions & Sanctions:

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:

School Actions & Sanctions-Pupils **Possible 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 e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X	X	X		X	X	X	X	X
Unauthorised use of mobile phone / digital camera / other mobile device	X	X	X			X		X	X
Unauthorised use of social media / messaging apps / personal email	X	X	X		X	X	X	X	X
Unauthorised downloading or uploading of files	X	X	X		X	X	X	X	X
Allowing others to access the School's network by sharing username and passwords	X	X	X		X	X	X	X	X
Attempting to access or accessing the School's network, using another Pupil's account	X	X	X		X	X	X	X	X
Attempting to access or accessing the School's network, using the account of a member of Staff	X	X	X		X	X	X	X	X
Corrupting or destroying the data of other users	X	X	X		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	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X	X
Actions which could bring the School into disrepute or breach the integrity of the ethos of the School	X	X	X		X	X	X	X	X
Using proxy sites or other means to subvert the School's filtering system	X	X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X	X	X	X

School Actions & Sanctions - Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Head teacher	Refer to designated safeguarding lead	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email (No risk to children).	X	X		X		X	X	X	X
Unauthorised downloading or uploading of files	X	X	X	X	X	X	X	X	X
Allowing others to access the School's network by sharing username and passwords or attempting to access or accessing the School's network, using another person's account	X	X	X	X	X	X	X	X	X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X	X	X		X	X	X	X
Deliberate actions to breach data protection or network security rules	X	X	X	X	X	X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X	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	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	X	X	X	X	X	X	X	X	X
Actions which could compromise the Staff member's professional standing	X	X	X	X	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	X	X	X
Using proxy sites or other means to subvert the School's filtering system	X	X	X	X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X		X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X		X			X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X	X

7. Pupil Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These 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. 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 digital 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.

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.

7.1 Acceptable Use Policy Agreement

All new pupils/parents are provided with a 'New Pupil School Agreement Booklet' which the pupil/parent has to read/sign – The responses are recorded on SIMS)

Pupil Acceptable Use 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.

Pupils are not permitted to store or publish any school work/examination work on the internet.

For my own personal safety:

• I understand that the school will monitor my use of the systems, devices and digital communications.

• I will keep my username and password safe and secure – I will not share it, 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 be aware of "stranger danger", when I am communicating on-line.

• I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.).

• I will not meet people off-line that I have only communicated with on-line.

• I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

• I understand that the school systems and devices are only intended for educational use only.

• 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 use the school systems or devices for on-line gaming unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

• I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

• I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

• I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

• I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

• I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to by-pass the filtering/security systems in place to prevent access to such materials.

• I will immediately report any damage or faults involving equipment or software, however this may have happened.

• I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, 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 not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

• I will not use social media sites at any time in school.

When using the internet for research, I recognise that:

• I should 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 try to download copies (including music and videos).

• When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

• I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Pupil Acceptable Use Agreement:

• I have read and understand the above and agree to follow these guidelines when:

• I use the school systems and devices (both in and out of school)

• I use my own devices in the school (when allowed) e.g. mobile phones, USB devices, cameras etc.

• I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.

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

I know that my son/daughter 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 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 Policy.

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 any concerns.

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 digital cameras provided by the school 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 GDPR and request parent's/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names. We respect everyone's privacy and in some cases protection, parents/carers are not allowed to record videos and digital images of their children at school events for their own personal use.

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.

I understand that I am not allowed to record videos or take digital images during school events.

Biometric Cashless Catering

In order to ensure maximum efficiency in taking payment for food we use a cashless system using biometrics for payment at the tills.

This system will significantly improve efficiency with benefits including:

· Improved security for handling cash transactions in the school

· Reduction in opportunities for bullying because there is nothing that can be stolen for use by another student

· Pupils will not have to remember to bring cash

· Reduction in queuing time

Students and staff will purchase their lunch and snacks by placing their index finger on the Biometric Reader. Payment is then deducted from their online account. School catering accounts can be topped up online using ParentPay. Students who qualify for FSM may also opt for the biometric system in order to continue to receive their lunch.

The biometric identification system in use at Philips High School uses the finger and its image to uniquely identify each person. The system measures many aspects of the finger to do this. Each student has their fingerprint registered, which will then be translated to a unique identification code which is entered into the system. The system does not create or store an image of the fingerprint.

When a student uses the biometric identification systems, they are identified by their identification code. This form of identification is called Biometrics, which translated means measurements of human characteristics. This is not finger-printing. The image of the fingerprint itself is not recorded or stored and cannot be regenerated from the digital data which cannot, therefore, be compared to existing records of fingerprint images. It is a system similar to that used on the latest iPhones.

We will not use the biometric information for any purpose other than school catering. Philips High School will store the biometric information collected securely in compliance with GDPR. We will only share this information with the suppliers of our biometric identification systems and will not unlawfully disclose it to any other person.

We must obtain parental consent to take and process biometric data from your child's finger and use this information for the purpose of providing your child with school catering. Attached to this booklet is a consent form which requires signing and returning to school to enable your child to use school catering. You can withdraw your consent at any time by writing to us. In addition, your child may at any time object or refuse to allow their biometric information to be used even if you have given your consent. We would appreciate it if could you explain this to your child.

If you do not wish your child's biometric information to be processed by the school, or your child objects to such pro-cessing, we will provide, where possible, reasonable alternative arrangements that allow them to access the relevant services.

Should you agree to the processing of your child's biometric information, please note that when he/she leaves Philips High, or if for some other reason he/she ceases to use the biometric system, his/her biometric data will be deleted.

8. Staff (and Volunteer) Acceptable Use Agreement

All new members of staff are required to sign the 'Policy Declaration Form' to confirm that they have read, understand and comply with the following Staff Acceptable Use Agreement:

Acceptable Use Agreement:

I understand that I must use the School's 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 as well as other users. I recognise the value of the use of ICT for enhancing learning and will ensure that 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 the use of the School's ICT systems (e.g. laptops, email, network etc.) out of School, and to the transfer of personal data (digital or paper based) out of School.
- I understand that the School's ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies, rules set down by the School.
- I will not disclose my 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 be professional in my communications and actions when using the School's 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 (e.g. on the School's website / Social Media) it will not be possible to identify personal information of those who are featured.
- I will only use chat and social networking sites in School in accordance with the *School's Social Media Policy*.
- I will only communicate with Pupils and Parents / Carers using official School systems, including the School's official Telephone Network. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The School and the Local Authority (LA) 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 (laptops / mobile phones / USB devices etc.) 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 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 understand 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 extremist material), inappropriate that 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 the School's 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's Data Protection 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 either the 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 Policy applies not only to my work and use of the School's 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 either 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 a warning, a suspension, referral to Governors and / or the LA and in the event of illegal activities the involvement of the Police.

9. School Technical Security Policy (including Filtering and Passwords)

9.1 Introduction:

Effective technical security depends not only on technical measures, but also on appropriate policies/ procedures, in addition to on good user education and training. The School is responsible for ensuring that the School's infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the School's policies).
- access to personal data is securely controlled in line with the School's Data Protection policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of the School's computer systems
- there is oversight from Senior Leaders that have impact on policy and practice.

9.2 Responsibilities:

The management of technical security will be the responsibility of Scott Fitton (Network Manager) whose work will be overseen by the SLT (Senior Leadership Team).

9.3 Technical Security Policy statements:

The School is responsible for ensuring that the School's infrastructure / network is as safe and secure as is reasonably possible. That policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will receive guidance/training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the School meets recommended technical requirements
- There will be regular reviews/audits of the safety and security of the School's technical systems
- Servers, wireless systems and cabling must be securely located with physical access restricted
- Appropriate security measures are in place (Smoothwall is our web filtering and firewall appliance. Microsoft Endpoint Protection is our antivirus/antimalware software. ABTutor is our Class Room management solution.) to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the School's systems and data.
- Responsibilities for the management of technical security are clearly assigned to the Network Manager.
- All users will have clearly defined access rights to the School's technical systems.
- Users who will be made responsible for the security of their username/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.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date. That regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Mobile device security and management procedures are in place.
- School Technical Staff will regularly monitor and record the activity of users on the School's technical systems with users being made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by Staff to control workstations and view user's activity.
- An agreed procedure is in place (Guests must sign and comply with the Staff Acceptable User Agreement) for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the School's system.
- The School's infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, Trojans etc.
- Personal data cannot be sent over the internet or taken off the School site unless safely encrypted or otherwise secured.

9.4 Password Security Policy Statements:

A safe and secure username / password system is essential if the above is to be established and will apply to all the School's technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

- All users will have clearly defined access rights to the School's technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Senior Leadership Team and Network Manager
- All the School's networks and systems will be protected by secure passwords that are regularly changed.
- The “master / administrator” passwords for the School's systems, used by the Technical Staff must also be available in a secure place e.g. the School safe. Consideration should also be given to using two factor authentication for such accounts.
- The School will never allow one user to have sole administrator access.
- Passwords for new users, and replacement passwords for existing users will be allocated by the Network Manager. Any changes carried out must be notified to the Network Manager.
- All users (adults and young people) will have responsibility for the security of their username/password. They 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.

9.5 Staff Passwords:

- All Staff users will be provided with a username/password by the Network Manager who will keep an up to date record of users and their usernames.
- The password should be a minimum of 8 characters long and must include: – uppercase character, lowercase character and a number.
- Passwords must not include proper names or any other personal information about the user that might be known by others.
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on.
- Passwords shall not be displayed on screen, and shall be securely hashed.

9.6 Student / Pupil Passwords

- All users will be provided with a username/password by the ICT Technical Team who will keep an up to date record of users and their usernames.
- Students are taught the importance of password security.
- The password should be a minimum of 8 characters long and must include: – uppercase character, lowercase character and a number.
- Passwords must not include proper names or any other personal information about the user that might be known by others.

9.7 Audit / Monitoring / Reporting / Review

The Network Manager will ensure that full records are kept of:

- User Ids
- User log-ons
- Security incidents related to this policy

9.8 Filtering Introduction:

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for E-Safety and acceptable use.

9.9 Responsibilities

The responsibility for the management of the School's Filtering procedure will be held by the Network Manager and his Team. They will manage the School's filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

9.10 Policy Statements:

Internet access is filtered for all users. Differentiated internet access is available for Staff and customised filtering changes are managed by the School. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged.

The Smoothwall System sends real time email alerts to the DSL and ADSLs in School if/when a user attempts to access inappropriate content. The following categories are used to generate real time email alerts and monitoring reports: Adult Content, Bullying, Criminal Activity, Radicalisation, Abuse, Substance Abuse and Suicide. Twice a week on a Monday and a Thursday, a member of the IT Technical Team will also email the weekly summary to the DSL (Designated Safeguarding Lead) and DDSLs (Deputy Designated Safeguarding Leads), which are then acted upon.

There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the School's Network, filtering will be applied that is consistent with School practice.

- The School manages its own filtering service
- The School has provided enhanced / differentiated user-level filtering through the use of the Smoothwall filtering programme.
- In the event of the Technical Staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by a member of the SLT.
- Mobile devices that access the School's internet connection will be subject to the same filtering standards as other devices on the School's systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from Staff for sites to be removed from the filtered list will be considered by the Network Manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed.

9.11 Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through their ICT lessons. They will also be warned of the consequences of attempting to subvert the filtering system.

Parents will be informed of the School's Filtering Policy through the *Child Protection and Safeguarding Policy.*

9.12 Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Network Manager who will decide whether to make School level changes (as above).

9.13 Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The School will therefore monitor the activities of users on the School's network and on School equipment as indicated in this policy and the *Acceptable Use Agreement.*

10. Links to other organisations or documents

Safer Internet Centre
Childnet
Professionals Online Safety Helpline
Internet Watch Foundation
http://ceop.police.uk/
ThinkUKnow

Curriculum:

Glow - http://www.educationscotland.gov.uk/usingglowandict/
Alberta, Canada - digital citizenship policy development guide.pdf
Teach Today – www.teachtoday.eu/
Insafe - Education Resources
Somerset - e-Sense materials for schools

Professional Standards / Staff Training:

DfE - Safer Working Practice for Adults who Work with Children and Young People
Kent - Safer Practice with Technology
Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs
Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support:

Somerset - Questions for Technical Support
NEN - Guidance Note - esecurity

Working with parents and carers:

Connect Safely - a Parents Guide to Facebook
Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers
DirectGov - Internet Safety for parents
Get Safe Online - resources for parents
Teach Today - resources for parents workshops / education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Insafe - A guide for parents - education and the new media
The Cybersmile Foundation (cyberbullying) - advice for parents