Online, Email, Internet and E-Safety Policy for Staff, Pupils, Parents and Governors (inclusive of Social Media Policy and Procedures)

As part of the Education Technology and computing program at Lowbrook, pupils are offered access to both Internet, email and VLE (Virtual Learning Environment) facilities. We believe that the Internet offers a wonderful environment for children to learn and have fun. However, we are mindful of the harm that can be caused to children online, including cyber bullying, pornography and the threat of radicalization. This policy is written in conjunction with the Lowbrook Social Media Policy and the Academy's Virtual Learning Protocol and Agreement in response to the COVID-19 pandemic, the schools behaviour, anti-bullying and the schools Safeguarding Policy. (**Appendix 13**).

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school Education Technology 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.

It is the school's number one priority to keep children safe and that includes whilst 'connected' and involved in our virtual environments. The school uses the September 2020 "Keeping Children Safe in Education" as a primary source for this policy (Annexe C, page 62).

The three categories of risk are as follows:

• content: being exposed to illegal, inappropriate or harmful material including radicalisation;

• contact: being subjected to harmful online interaction with other users; and

• conduct: personal online behaviour that increases the likelihood of, or causes, harm

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

Governors:
Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training and the requirement to ensure children are taught about safeguarding, including online, that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach. The Governors are responsible for ensuring this policy is regularly updated and reflects the practice within the school.

Principal and Senior Leaders:
The Senior Leadership Team is responsible for the approval of this Policy and for reviewing the effectiveness of the policy. This will be carried out having receiving regular information about online incidents and monitoring reports.

- Regular meetings with the E-Safety Leader-Raman Herr.
- Regular monitoring of e-safety incident logs.
- The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Leader.
- The Principal and the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse"). The Safeguarding policy may be used alongside this policy.
- The Senior Leaders are responsible for ensuring that the E-Safety Leader and other relevant staff receive suitable guidance to enable them to carry out their e-safety roles as relevant.
- The Principal/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 those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Leader.
- Cyber Support E- Mail to the Principal alerting him to web traffic events that violate our policy. (E-mails provided by Microsoft and the Smoothwall Firewall are managed by Syber Support). The Principal would be informed by Cyber Support immediately if there was a serious breach e.g. multiple attempts to access an inappropriate website by a single user (see Prevent Risk Assessment, Lowbrook Child Protection and Safeguarding Policy 2021).

E-Safety Leader:
Harriet Daniels

- 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 advice and training for staff.
- Liaises with school with Cyber Support, our technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Reports regularly to Senior Leadership Team.

Network Manager:
Cyber Support
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 E-Safety Policy/Guidance that may apply.

- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- To ensure that the Academy has appropriate filters and monitoring systems in place to limit children's exposure to the three areas of risk from the school's IT system. (Three Areas of Risk are defined as **Content**: being exposed to illegal, inappropriate or harmful material; **Contact**: being subjected to harmful online interaction with other users; **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm (Keeping Children Safe in Education September 2020). The UK Safer Internet Centre has published guidance as to what appropriate looks like (UK Safer Internet Centre: Appropriate Filtering & Monitoring). Commerce: risks such as online gambling, inappropriate advertising and phishing.
- To ensure that a reporting mechanism is in place and it is maintained. Report inappropriate content for access or blocking. Cyber Support send an automated weekly E- Mail to P Reid (School Business Manager, DDSL, Prevent Trainer), D Rooney (Principal, DSL), R Herr alerting the Academy to web traffic events that violate our policy. (E-mails provided by Microsoft and managed by Cyber Support. Cyber Support would inform the Academy immediately if there was a serious breach e.g. single and multiple attempts to access an inappropriate website by a single user. See Prevent Risk Assessment, Lowbrook Child Protection and Safeguarding Policy 2021
- To advise the Academy on the above points so that the Academy can do all that it reasonably can to limit children's exposure to risks from its IT system as required by the Prevent Duty.

Teaching and Support Staff
are responsible for ensuring that:

- They report any suspected misuse or problem to the Principal/ E-Safety Leader. This will follow a 3 step plan: **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 (Identified on the curriculum map).
- Pupils understand and follow the e-safety and acceptable use policies.
- 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.
- Ensure that they always directly or remotely supervise children whilst using technology including the Internet.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Safeguarding Officers:
Dave Rooney, Harriet Daniels, Veronica Quinby and Paula West should be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data.
- Access to inappropriate materials (including pornography and material that poses a threat of radicalisation).
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

- Ensure that the Academy has appropriate filters and monitoring systems in place to limit children's exposure to the three areas of risk from the school's IT system in line with Prevent Duty.

Pupils:

- Are responsible for using the school digital technology systems in accordance with the behaviour policy of class rules and SIDS Top Tips .
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- 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.
- Should understand that the Academy has monitoring and filtering systems in place and that access and usage is carefully scrutinised.
- Should understand that inappropriate use outside of school can and will be dealt with under school policies.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature and workshops delivered. 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.
- Their children's personal devices in the school (e.g. KS2 Kindle Fire).
- Appropriate support on usage of our remote learning platform outlined in our Remote Learning Protocol and Agreement in response to COVID-19.
- Reinforcing SIDS Top Tips **(appendix 17).**
- Reinforcing the practices regarding: Content, Context and Conduct.

Policy Statements

Education – pupils

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

The use of technology has become a significant component of many safeguarding issues. Commerce abuse, Child sexual exploitation; radicalisation; sexual predation, sexting and up skirting: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

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

- A planned e-safety curriculum is provided as part of Computing / Physical and Emotional Health lessons: other lessons and should be regularly revisited across Domain areas and daily use., (Plans are available for each Year Group on the Staff Server) and identified within the whole school progression matrix.

- Key e-safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices. All children are taught to abide by SIDS top tips. **(Appendix 17)**
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day with Paul Hay
- Reference to the relevant web sites / publications e.g. www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers https://www.lowbrookacademy.co.uk/ (see appendix for further links / resources)

✓ A dedicated e-safety tab is available on the school's website

Education & Training – Staff / Volunteers

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

- A planned programme of formal e-safety training (Paul Hay, PCLS Training) will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out annually or where necessary.
- The E-Safety Leader/ Officer (or other nominated person) will receive regular updates through attendance at external training events (e.g. from LA, Paul Hay or other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Leader/ Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

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- Cyber Support are contacted by the school to undertake this work.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted (locked server room).
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and password. (This is not to be shared).
- The "master / administrator" passwords for the school Education Technology system, used by the Network Manager (or other person) must also be available to the I.T. Leader Raman Herr and the Principal.
- Cyber Support are employed and responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and monitored. There is a clear process in place to deal with requests for filtering changes. Cyber Support and Raman Herr manage this and can be contacted if additional filtering of cites is required.
- The school has provided enhanced / differentiated user-level filtering.
- School technical staff (Cyber Support) regularly monitor and record the activity of users on the school technical systems in accordance with DFE Guidance. https://www.gov.uk/government/news/new-measures-to-keep-children-safe-online-at-school-and-at-home Users are made aware of this in the Acceptable Use Agreement
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software. This service is provided by Cyber Support.
- An agreed policy is in place for the provision of temporary access of guests (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *pupils* in the digital / video images.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, Twitter 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 without permission. On occasion newspaper and associated press like to use names. (This will only happen if permission is expressly granted).
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website twitter or other digital medium.
- Pupil's work can be published with the permission of the Academy.

Use of Mobile Phones and Digital Photography Policy

Pupils may their photographs taken to provide evidence of their achievements for their development records. Staff, visitors, volunteers and students are not permitted to use their own mobile phones to take or record any images of the Academy's children for their own records during the school day.

Procedures

1. Under the GDPR Act 2018, the Academy must seek parental consent to take photographs and use video recorders.

2. Photographs may be taken during indoor and outdoor play and learning and displayed in the academy and in albums or a pupil's development records for children and parent carers, governors, OFSTED, LA officers, to look through.

3. Often photographs may contain other pupils in the background.

4. Events such as Sports Day, outings, Christmas and fundraising events may be recorded by video and photographs by staff and parent/carers but always in full view of all attending. They are explicitly informed that it is of their own children and not to be published on ay social media platform.

5. Parents/careers must not post photographs or video containing other pupils taken at the academy's events on social media websites.

6. On occasion, the academy might like to use photographs of pupils taking part in an activity to advertise/promote the academy via the website. In this instance, specific parental permission will be required, and is sought in the September Data processing permissions forms.

7. Visitors may only use their phones outside the building or in the VLE during non-contact time and should be challenged if seen using a camera inappropriately or photographing children.

8. The use of cameras, iPads and mobile phones are prohibited in toilet areas.

9. All academy cameras and videos should be kept securely at all times and used with appropriate authority.

Prevent Duty

From 1 July 2015 all schools are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015 (“the CTSA 2015”), in the exercise of their functions, to have “due regard to the need to prevent people from being drawn into terrorism”. This duty is known as the Prevent duty.

The Academy has undertaken a risk assessment of our pupils being drawn into terrorism. This means being able to demonstrate both a general understanding of the risks affecting children and young people within our local area and a specific understanding of how to identify individual children who may be at risk of radicalisation and what to do to support them. RBWM is considered a low risk LA. All staff and Governors have received Training in the Prevent Duty. Two members of staff are Home Office accredited trainers.

Schools must ensure that children are safe from terrorist and extremist material when accessing the internet in schools. The Academy follows the advice from The Department for Education advice for schools on the Prevent duty, June 2015
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and it is based on guidance published by the Information Commissioners office and model privacy notices published y the Department for Education. It also takes into account the expected provisions of the General Data Protection Regulations (GDPR) as of April 2018. Personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject’s rights
- Secure.
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.
- It has a Data Protection Policy & Privacy Notice
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

- There is a policy for reporting, logging, managing and recovering from information risk incidents

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse. It could be a minimum fine of £500,000 if the school in in breach of this.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data. All computers and keys are locked or securely encrypted.

Communications

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

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

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the E-safety leader (Raman Herr) or a member of the SLT – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email) must be professional in tone and content.

- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies. Again, SIDs top tips are taught across the school.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

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

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 personal social media to pupils, parents / careers 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 minimize risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the e-safety coordinator to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies. Full guidance for social media use is referred to in Appendix 13 of this policy.

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
	pornography				X	
	promotion of any kind of discrimination				X	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	X		
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. You Tube		X			

Lowbrook Child Protection Policy 2021 details how the school IT system is monitored and filtered. It also contains a list of content that is automatically blocked.

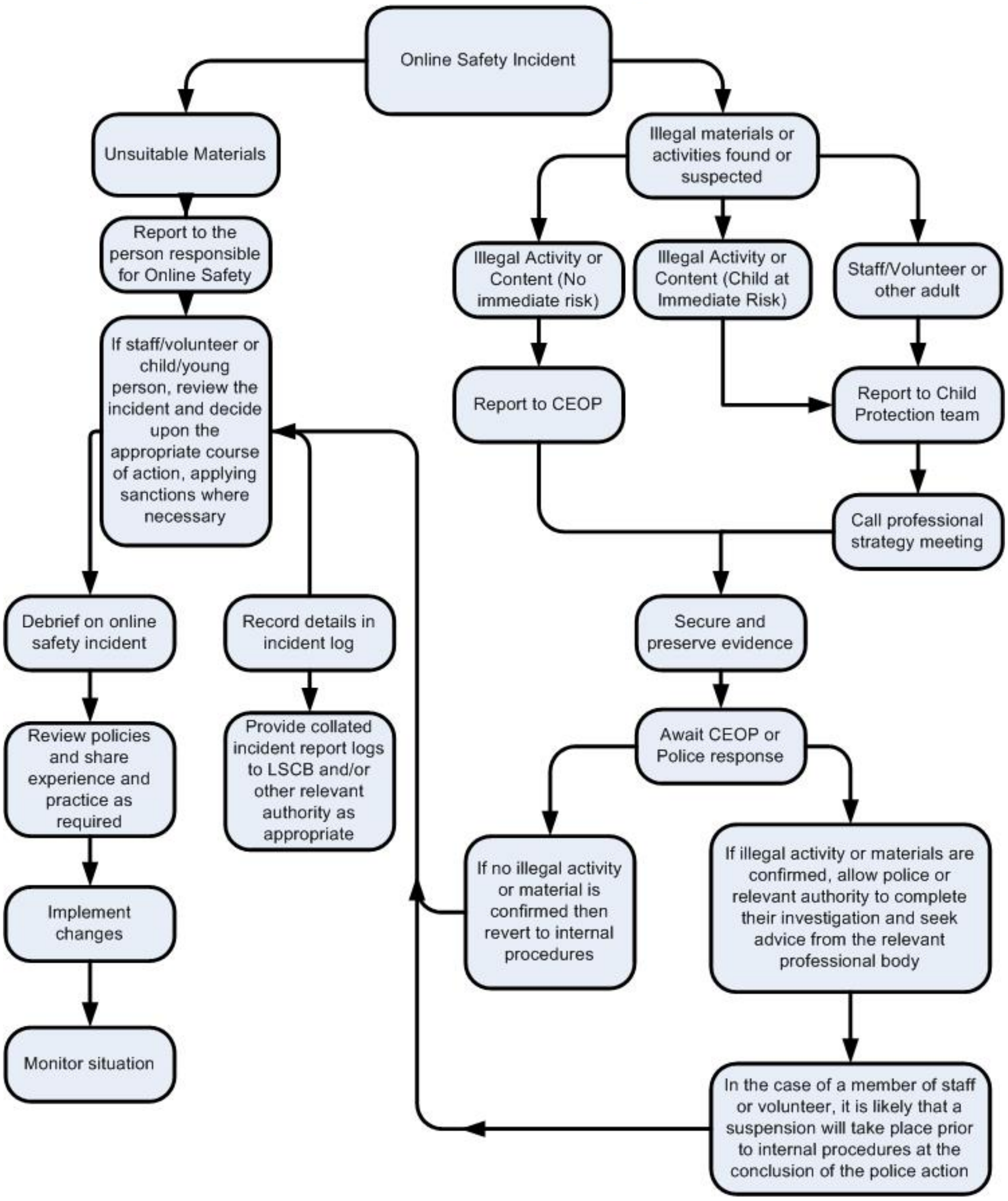
Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the school safeguarding officer and police.

Lowbrook Academy



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
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as 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 CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or 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 prior to internal procedures at the conclusion of the police action

Other Incidents

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures.
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action.
- If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour.
    - the sending of obscene materials to a child.
    - adult material which potentially breaches the Obscene Publications Act.
    - criminally racist material.
    - other criminal conduct, activity or materials.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation. Do not view the content or images. You have the right to confiscate phones and devices if you are investigating abuse.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school 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:

Pupils **Actions / Sanctions**

Incidents:	Refer to class teacher	Refer to the Principal/E-safety leader	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Warning	Further sanction e.g. 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
Unauthorised use of non-educational sites during lessons	x	x				x	
Unauthorised use of mobile phone/digital camera / other mobile device	x	x			x		
Unauthorised use of social media/messaging apps / personal email	x	x			x		
Unauthorised downloading or uploading of files	x	x		x			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x			x	x	
Continued infringements of the above, following previous warnings or sanctions	x	x			x	x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	x			x	x	x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x		x	x	x	
Deliberately accessing or trying to access offensive or pornographic material	x	x		x	x	x	x

Staff **Actions / Sanctions**

Incidents:	Refer to the Principal	Refer to HR (Strictly Education)	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X		X	X
Inappropriate personal use of the internet/social media /personal email	x				x		x
Unauthorised downloading or uploading of files	x			x			
Deliberate actions to breach data protection or network security rules	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
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	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		
Actions which could compromise the staff member's professional standing	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
Using proxy sites or other means to subvert the school's filtering system	x	x		x	x	x	x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x		x	x		x
Deliberately accessing or trying to access offensive or pornographic material	x	x		x	x	x	x
Breaching copyright or licensing regulations	x	x		x	x		
Continued infringements of the above, following previous warnings or sanctions	x	x	x	x	x	x	x

Signed: Chair of Governors

Signed: Principal

Lowbrook Academy

Appendix 1

Pupil Acceptable Use Policy Agreement – KS2

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer/iPads/devices and other equipment

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

I know that the school has a system that checks all the websites that I go on to.

I agree to not use my school email or Google Classroom account for non-school use.

I agree to never give my personal details when using the internet.

I agree to use online apps and communication at school or at home in line with school rules and know the school can sanction me if I don't.

I know that if I break the rules I might not be allowed to use a computer or device and school sanctions may apply.

Signed (child):……………………………………………

Lowbrook Academy

Appendix 2

Staff, Governors (and Volunteer) Acceptable Use Policy Agreement

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

This Acceptable Use Policy is intended to ensure:

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

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

Acceptable Use Policy Agreement
I understand that I must use school Education Technology systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the Education Technology systems and other users. I recognise the value of the use of Education Technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of Education Technology . I will, where possible, educate the young people in my care in the safe use of Education Technology 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 Education Technology systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school Education Technology systems (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school Education Technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person (Mr Rooney).

I will be professional in my communications and actions when using school Education Technology 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 website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with pupils and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)
- I will not engage in any on-line activity that may compromise my professional responsibilities as outlined in this policy.

The Academy has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs / laptops / mobile phones / 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 use personal email addresses on the school Education Technology systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies or agreed by Mrs Herr or Mr Rooney.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school Education Technology equipment in school, but also applies to my use of school Education Technology systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that illegal online activity outside of school will be dealt with via the school's disciplinary procedures and/or the schools Child Protection policy.
- 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 Local Authority and in the event of illegal activities the involvement of the police.

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

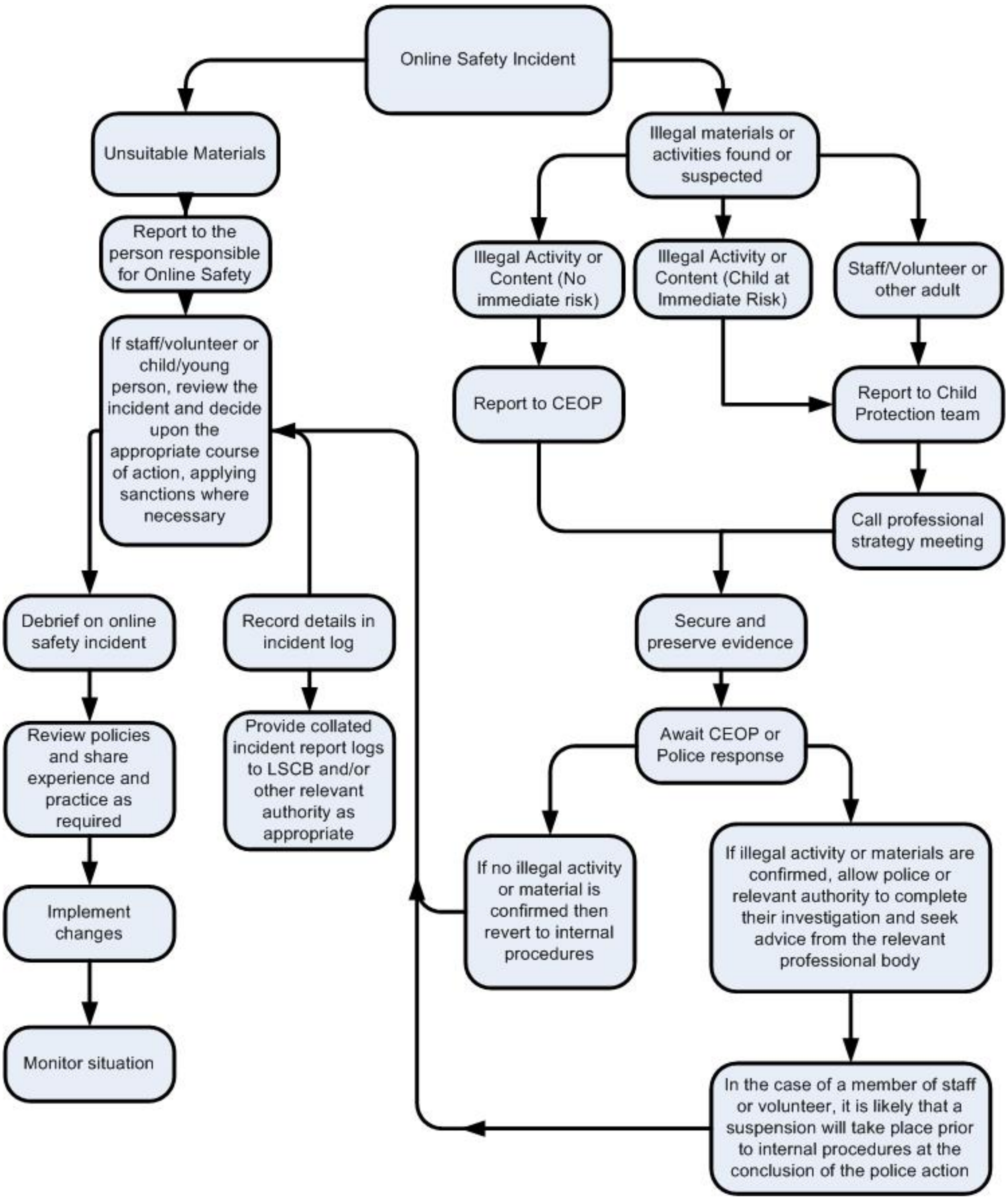
Staff/Volunteer Name

Signed

Date

Appendix 3

Responding to incidents of misuse – flow chart


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
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as 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 CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or 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 prior to internal procedures at the conclusion of the police action

Lowbrook Academy

Appendix 4

Record of Reviewing Sites (for internet misuse)

Name	
Position	
Signature	

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

Group	
Date	
Reason for investigation	

Details of first reviewing person

Details of second reviewing person

Name	
Position	
Signature	

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

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Appendix 5

School Reporting Log Template

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

Appendix 6

School Training Needs Audit Template

<table>
<tr><td colspan="7">Training Needs Audit Log
Group .... Date ....</td></tr>
<tr><td>Name</td><td>Position</td><td>Relevant training in last 12 months</td><td>Identified training need</td><td>To be met by:</td><td>Cost</td><td>Review date</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Appendix 7

School Technical Security Policy (including filtering and passwords)

Introduction

The school is responsible for ensuring that the school 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-This is determined by the SLT in the IT staff drive.
- 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 school computer systems. These are completed daily by Cyber Support.
- There is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security outsourced to Cyber Support and is managed by the E-Safety lead Raman Herr who reports directly to the Principal.

Technical Security

Policy statements

The school ensures that the infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It also ensures that the relevant people will receive guidance and 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 and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place 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 systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff (Cyber Support).
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff (Cyber Support) and will be reviewed, at least annually.
- 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.
- Cyber Support are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Mobile device security and management procedures are in place
- Cyber Support monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system (Smoothwall Safeguarding) is in place for users to report any actual / potential technical incident to the E-Safety Leader/Principal.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school. Please refer to the Staff Handbook.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.. Our Anti-Viral software is managed by Cyber Support.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices and email.

Policy Statements

- All users will have clearly defined access rights to school 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.
- All school networks and systems will be protected by secure passwords that are regularly changed
- The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the Principal or other nominated senior leader and kept in a secure place e.g. school safe. The school uses two factor authentications for such accounts where this facility is possible.
- Passwords for new users, and replacement passwords for existing users will be allocated by Cyber Support. Any changes carried out must be notified to the manager of the password security policy-Raman Herr.
- All users (adults and young people) will have responsibility 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.

Staff passwords:

- **All staff users will be provided with a username and password** by Cyber Support 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 three of – uppercase character, lowercase character, number, special characters
- the account should be "locked out" following six successive incorrect log-on attempts
- 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 (use of one-way encryption)
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- should be different for systems used inside and outside of school

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction,
- through the school's e-safety policy and password security policy,
- through the Acceptable Use Agreement.

Pupils will be made aware of the school's password policy:

- in lessons,
- through the Acceptable Use Agreement.

Audit / Monitoring / Reporting / Review

The responsible person (Mrs Raman Herr) will ensure that full records are kept of:

- User Ids and requests for password changes,
- User log-ons,
- Security incidents related to this policy.

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. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by Cyber Support. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

All users have a responsibility to report immediately to the E-safety lead Mrs Herr any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

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.

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 and Cyber Support. Illegal content is filtered by the 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 and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system.

- The school maintains and supports the managed filtering service provided by the Internet Service Provider
- 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 the Principal.
- 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 technical staff. If the request is agreed, this action will be recorded.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- staff meetings, briefings, Inset.

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 E-safety Coordinator who will decide whether to make school level changes.

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 network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use Agreement.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- E-Safety Coordinator
- Senior Leadership Team
- Cyber Support/ Local Authority / Police on request

Lowbrook
Academy

Appendix 8

School Personal Data Handling (To be read in conjunction with the school's General Data Protection Policy, Freedom of Information Policy and the school's Privacy Notice).

School Personal Data Handling Policy

Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance.

Policy Statements

The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

The school has a clear and regularly updated and monitored GDPR policy and associated procedures.

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil progress records, reports
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Responsibilities

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Training & awareness
All staff will be made aware of their responsibilities, as described in this policy through:

- Staff meetings / briefings / Inset,
- Day to day support and guidance from Senior Leaders,
- Understanding of the schools GDPR policy and procedures.

Secure Storage of and access to data
The school will ensure that Education Technology systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes. All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media (server back-up hard drives). Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected (this will be supplied by the school only),
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. This is managed by Cyber Support.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

Secure transfer of data and access out of school
The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- If secure remote access is not possible, with the permission of the SLT users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;

- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software. Cyber Support's approval is required.

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data. Data disposal is conducted by Cyber Support on behalf of the school.

Lowbrook Academy

Appendix 9

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.
It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990
This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;

- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child

also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

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.

The Education and Inspections Act 2011
Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.
http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

The Protection of Freedoms Act 2012
Requires schools to seek permission from a parent / carer to use Biometric systems

The Data Protection Act 2018

The Data Protection Act 2018 is the UK's implementation of the **General Data Protection Regulation** (**GDPR**).

Voyeurism (Offences Act) 2019

The School Information Regulations 2012

Requires schools to publish certain information on its website.

Working together to Safeguard Children 2023

KCSIE 2024

Appendix 10

Links to other organisations or documents

The following links may help those who are developing or reviewing a school e-safety policy.

UK Safer Internet Centre

Safer Internet Centre

South West Grid for Learning

Childnet - www.childnet.com/cyberbullying-guidance

Professionals Online Safety Helpline

Internet Watch Foundation

CEOP

http://ceop.police.uk/

http://www.thinkuknow.co.uk/

Others:

INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm

UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis

Guide for Parents - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/490001/Social_Media_Guidance_UKCCIS_Final_18122015.pdf.pdf

Netsmartz - http://www.netsmartz.org/index.aspx

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.pshe-association.org.uk

www.educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Support for Schools

Specialist help and support SWGfL BOOST

Cyberbullying

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government Better relationships, better learning, better behaviour

DCSF - Cyberbullying guidance

DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

Social Networking

Digizen – Social Networking

SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people

Connectsafely Parents Guide to Facebook

Facebook Guide for Educators

Curriculum

SWGfL Digital Literacy & Citizenship 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

Data Protection

Information Commissioners Office:

Your rights to your information – Resources for Schools - ICO

ICO pages for young people

Guide to Data Protection Act - Information Commissioners Office

Guide to the Freedom of Information Act - Information Commissioners Office

ICO guidance on the Freedom of Information Model Publication Scheme

ICO Freedom of Information Model Publication Scheme Template for schools (England)

ICO - Guidance we gave to schools - September 2012 (England)

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Hosted Services

Information Commissioners Office good practice note on taking photos in schools

ICO Guidance Data Protection Practical Guide to IT Security

ICO – Think Privacy Toolkit

ICO – Personal Information Online – Code of Practice

ICO – Access Aware Toolkit

ICO Subject Access Code of Practice

ICO – Guidance on Data Security Breach Management

SWGfL - Guidance for Schools on Cloud Hosted Services

LGfL - Data Handling Compliance Check List

Somerset - Flowchart on Storage of Personal Data

NEN - Guidance Note - Protecting School Data

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

SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum

SWGfL BOOST Presentations - parents presentation

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

Research

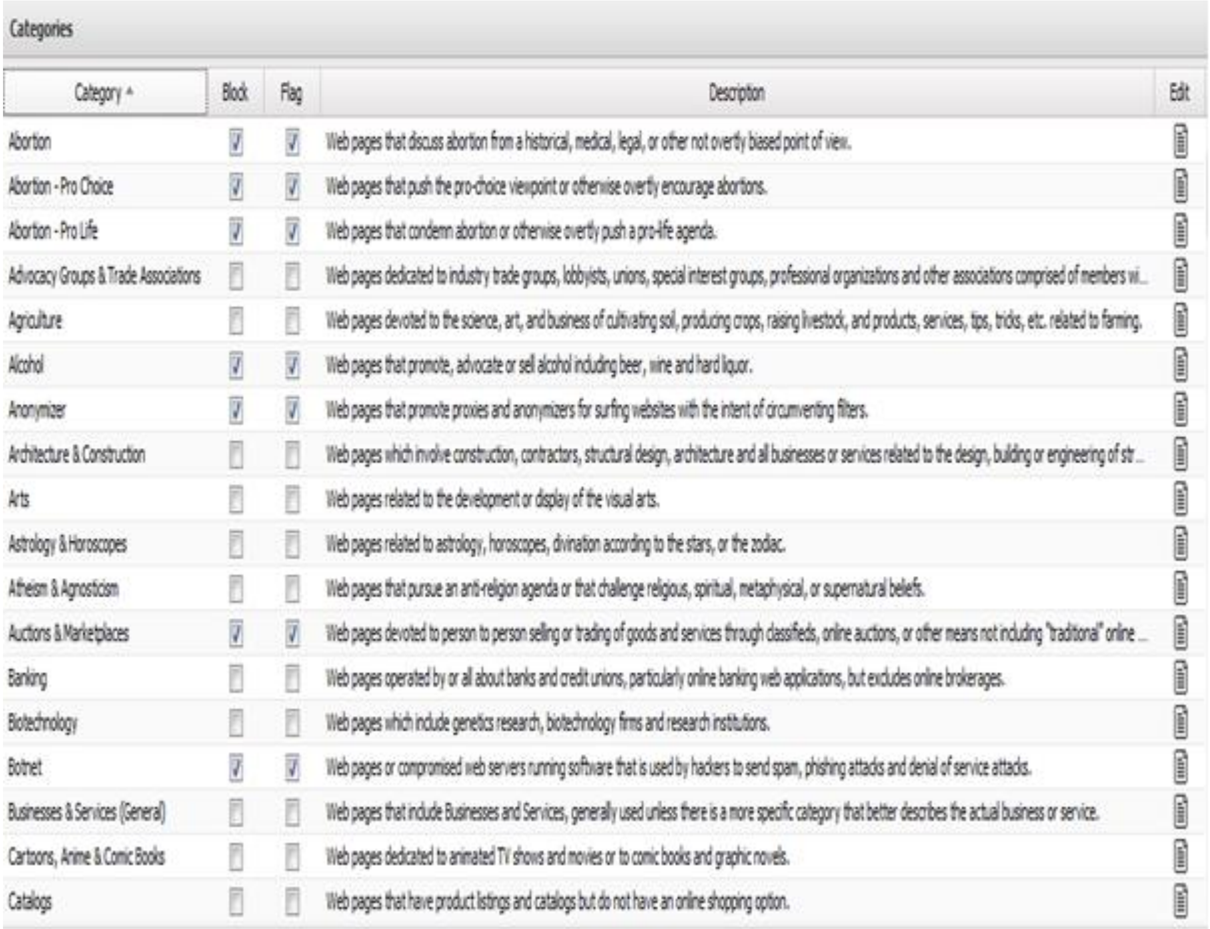
EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011

Futurelab - "Digital participation - its not chalk and talk any more!"

Lowbrook Academy

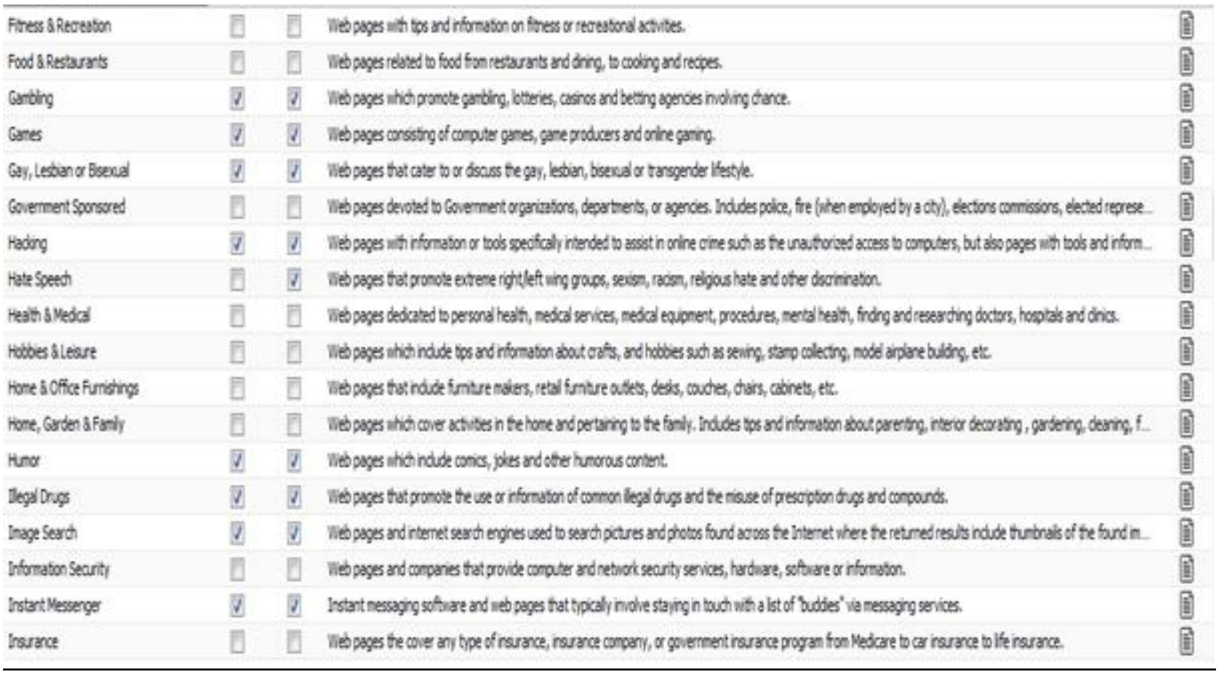
Appendix 11

List Web Filtering Categories

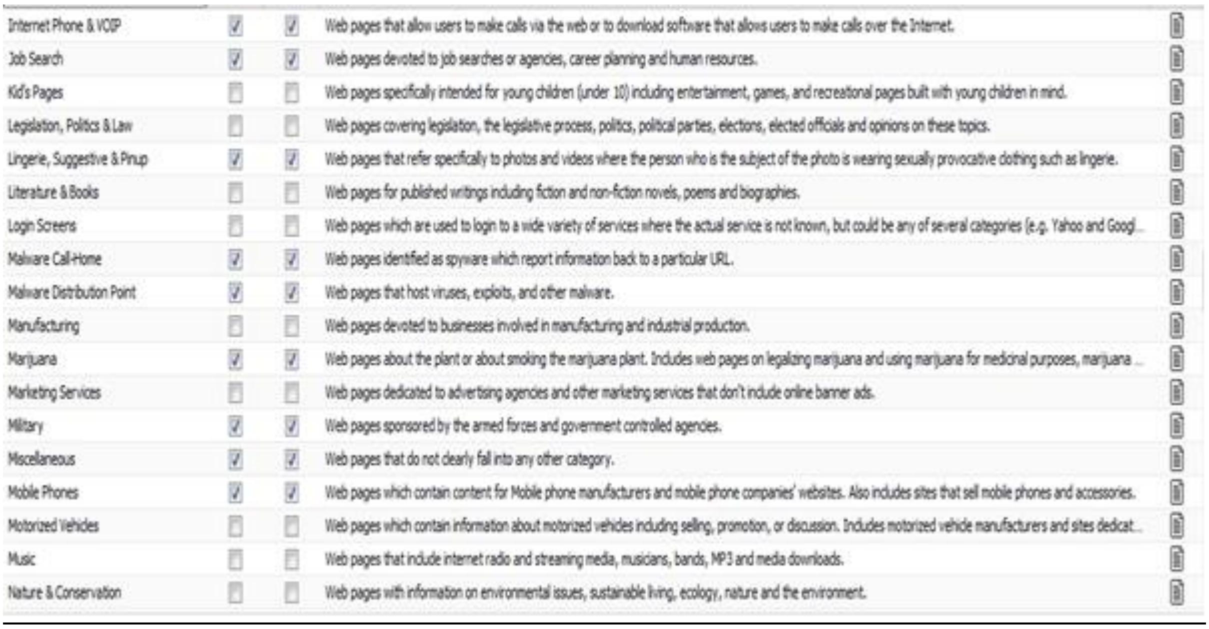


Categories

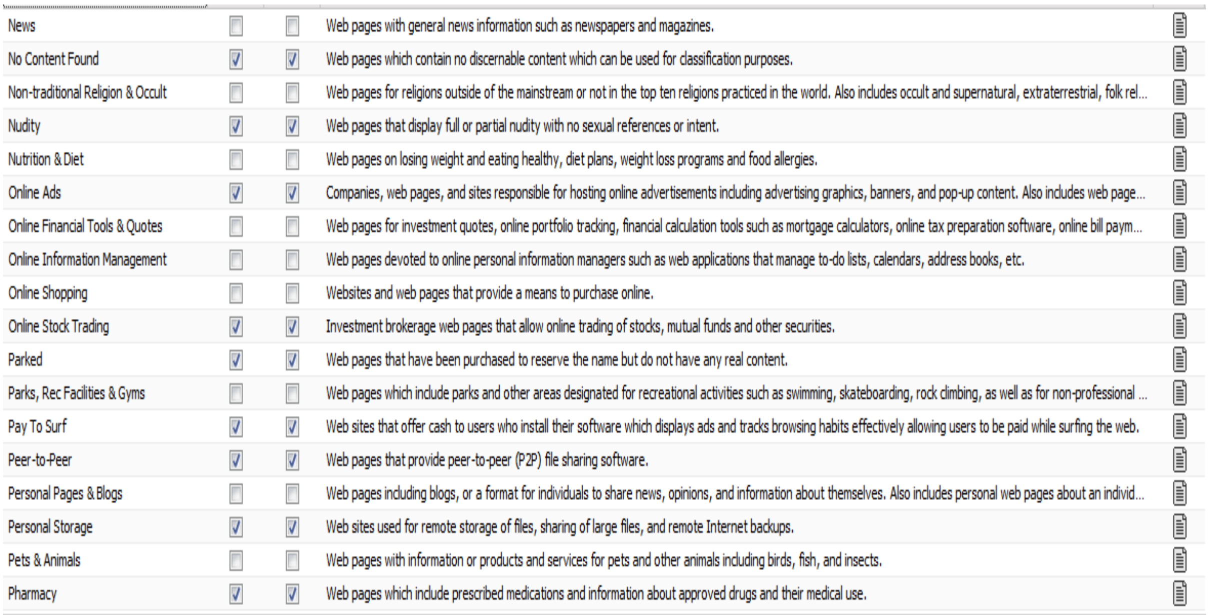
Category ▲	Block	Flag	Description	Edit
Abortion	☑	☑	Web pages that discuss abortion from a historical, medical, legal, or other not overtly biased point of view.	🗎
Abortion - Pro Choice	☑	☑	Web pages that push the pro-choice viewpoint or otherwise overtly encourage abortions.	🗎
Abortion - Pro Life	☑	☑	Web pages that condemn abortion or otherwise overtly push a pro-life agenda.	🗎
Advocacy Groups & Trade Associations	□	□	Web pages dedicated to industry trade groups, lobbyists, unions, special interest groups, professional organizations and other associations comprised of members wi...	🗎
Agriculture	□	□	Web pages devoted to the science, art, and business of cultivating soil, producing crops, raising livestock, and products, services, tips, tricks, etc. related to farming.	🗎
Alcohol	☑	☑	Web pages that promote, advocate or sell alcohol including beer, wine and hard liquor.	🗎
Anonymizer	☑	☑	Web pages that promote proxies and anonymizers for surfing websites with the intent of circumventing filters.	🗎
Architecture & Construction	□	□	Web pages which involve construction, contractors, structural design, architecture and all businesses or services related to the design, building or engineering of str...	🗎
Arts	□	□	Web pages related to the development or display of the visual arts.	🗎
Astrology & Horoscopes	□	□	Web pages related to astrology, horoscopes, divination according to the stars, or the zodiac.	🗎
Atheism & Agnosticism	□	□	Web pages that pursue an anti-religion agenda or that challenge religious, spiritual, metaphysical, or supernatural beliefs.	🗎
Auctions & Marketplaces	☑	☑	Web pages devoted to person to person selling or trading of goods and services through classifieds, online auctions, or other means not including "traditional" online ...	🗎
Banking	□	□	Web pages operated by or all about banks and credit unions, particularly online banking web applications, but excludes online brokerages.	🗎
Biotechnology	□	□	Web pages which include genetics research, biotechnology firms and research institutions.	🗎
Botnet	☑	☑	Web pages or compromised web servers running software that is used by hackers to send spam, phishing attacks and denial of service attacks.	🗎
Businesses & Services (General)	□	□	Web pages that include Businesses and Services, generally used unless there is a more specific category that better describes the actual business or service.	🗎
Cartoons, Anime & Comic Books	□	□	Web pages dedicated to animated TV shows and movies or to comic books and graphic novels.	🗎
Catalogs	□	□	Web pages that have product listings and catalogs but do not have an online shopping option.	🗎



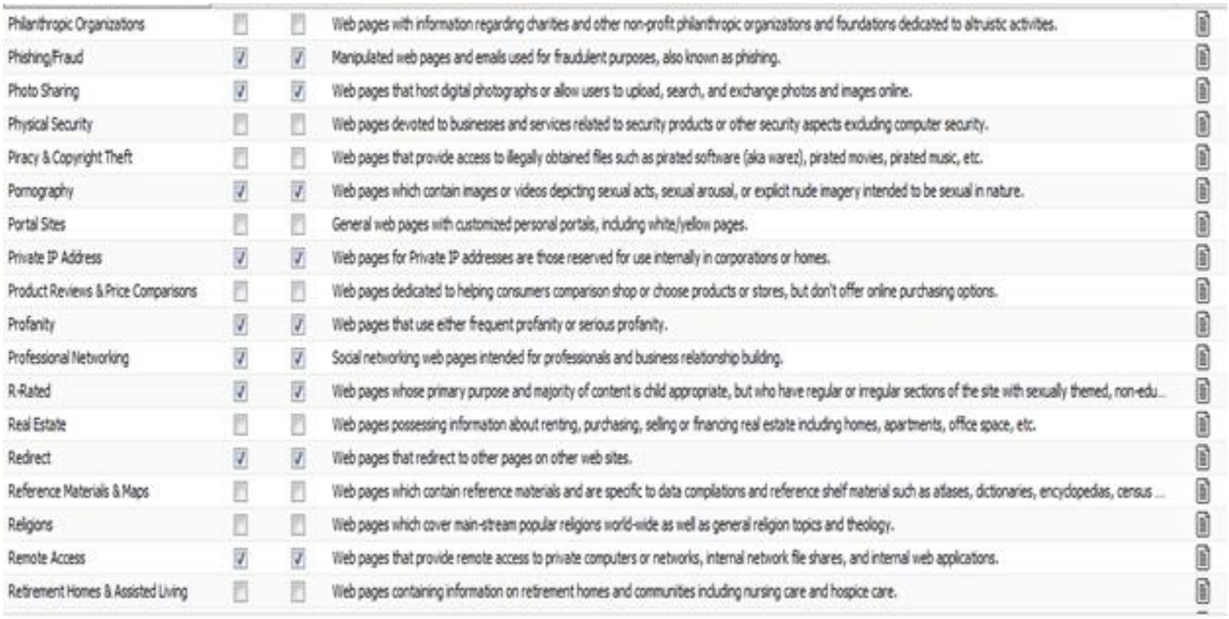
Fitness & Recreation	□	□	Web pages with tips and information on fitness or recreational activities.
Food & Restaurants	□	□	Web pages related to food from restaurants and dining, to cooking and recipes.
Gambling	☑	☑	Web pages which promote gambling, lotteries, casinos and betting agencies involving chance.
Games	☑	☑	Web pages consisting of computer games, game producers and online gaming.
Gay, Lesbian or Bisexual	☑	☑	Web pages that cater to or discuss the gay, lesbian, bisexual or transgender lifestyle.
Government Sponsored	□	□	Web pages devoted to Government organizations, departments, or agencies. Includes police, fire (when employed by a city), elections commissions, elected represe...
Hacking	☑	☑	Web pages with information or tools specifically intended to assist in online crime such as the unauthorized access to computers, but also pages with tools and inform...
Hate Speech	□	☑	Web pages that promote extreme right/left wing groups, sexism, racism, religious hate and other discrimination.
Health & Medical	□	□	Web pages dedicated to personal health, medical services, medical equipment, procedures, mental health, finding and researching doctors, hospitals and clinics.
Hobbies & Leisure	□	□	Web pages which include tips and information about crafts, and hobbies such as sewing, stamp collecting, model airplane building, etc.
Home & Office Furnishings	□	□	Web pages that include furniture makers, retail furniture outlets, desks, couches, chairs, cabinets, etc.
Home, Garden & Family	□	□	Web pages which cover activities in the home and pertaining to the family. Includes tips and information about parenting, interior decorating , gardening, cleaning, f...
Humor	☑	☑	Web pages which include comics, jokes and other humorous content.
Illegal Drugs	☑	☑	Web pages that promote the use or information of common illegal drugs and the misuse of prescription drugs and compounds.
Image Search	☑	☑	Web pages and internet search engines used to search pictures and photos found across the Internet where the returned results include thumbnails of the found im...
Information Security	□	□	Web pages and companies that provide computer and network security services, hardware, software or information.
Instant Messenger	☑	☑	Instant messaging software and web pages that typically involve staying in touch with a list of "buddies" via messaging services.
Insurance	□	□	Web pages the cover any type of insurance, insurance company, or government insurance program from Medicare to car insurance to life insurance.



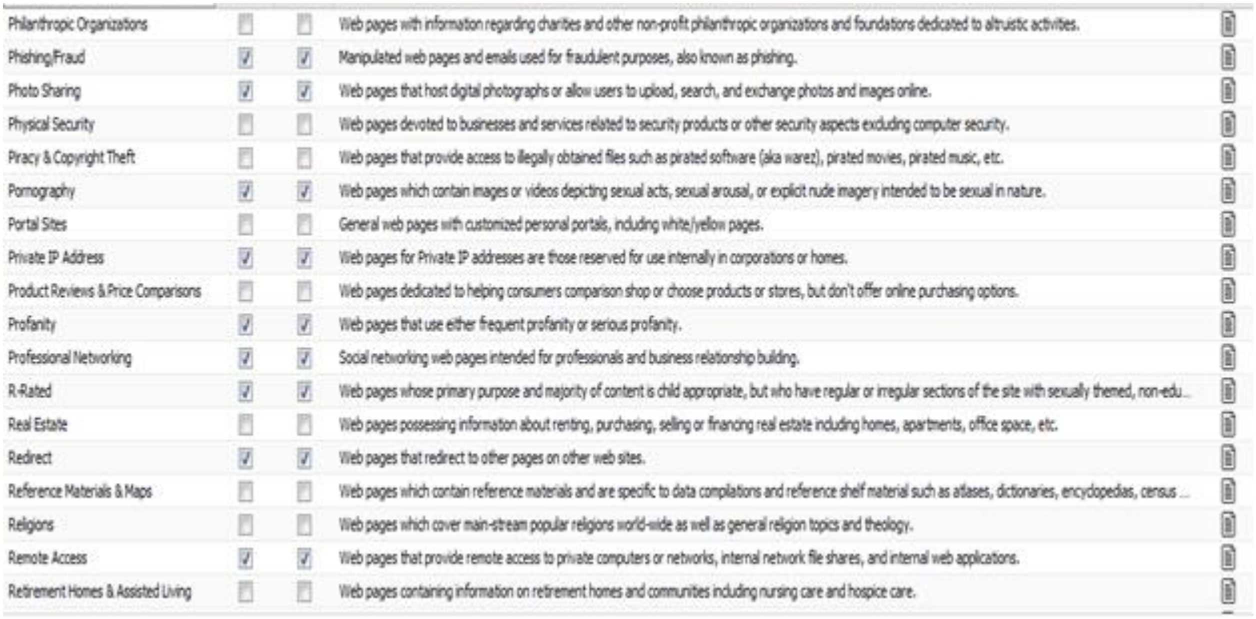
Internet Phone & VOIP	☑	☑	Web pages that allow users to make calls via the web or to download software that allows users to make calls over the Internet.
Job Search	☑	☑	Web pages devoted to job searches or agencies, career planning and human resources.
Kid's Pages	□	□	Web pages specifically intended for young children (under 10) including entertainment, games, and recreational pages built with young children in mind.
Legislation, Politics & Law	□	□	Web pages covering legislation, the legislative process, politics, political parties, elections, elected officials and opinions on these topics.
Lingerie, Suggestive & Pinup	☑	☑	Web pages that refer specifically to photos and videos where the person who is the subject of the photo is wearing sexually provocative clothing such as lingerie.
Literature & Books	□	□	Web pages for published writings including fiction and non-fiction novels, poems and biographies.
Login Screens	□	□	Web pages which are used to login to a wide variety of services where the actual service is not known, but could be any of several categories (e.g. Yahoo and Googl...
Malware Call-Home	☑	☑	Web pages identified as spyware which report information back to a particular URL.
Malware Distribution Point	☑	☑	Web pages that host viruses, exploits, and other malware.
Manufacturing	□	□	Web pages devoted to businesses involved in manufacturing and industrial production.
Marijuana	☑	☑	Web pages about the plant or about smoking the marijuana plant. Includes web pages on legalizing marijuana and using marijuana for medicinal purposes, marijuana ...
Marketing Services	□	□	Web pages dedicated to advertising agencies and other marketing services that don't include online banner ads.
Military	☑	☑	Web pages sponsored by the armed forces and government controlled agencies.
Miscellaneous	☑	☑	Web pages that do not clearly fall into any other category.
Mobile Phones	☑	☑	Web pages which contain content for Mobile phone manufacturers and mobile phone companies' websites. Also includes sites that sell mobile phones and accessories.
Motorized Vehicles	□	□	Web pages which contain information about motorized vehicles including selling, promotion, or discussion. Includes motorized vehicle manufacturers and sites dedicat...
Music	□	□	Web pages that include internet radio and streaming media, musicians, bands, MP3 and media downloads.
Nature & Conservation	□	□	Web pages with information on environmental issues, sustainable living, ecology, nature and the environment.



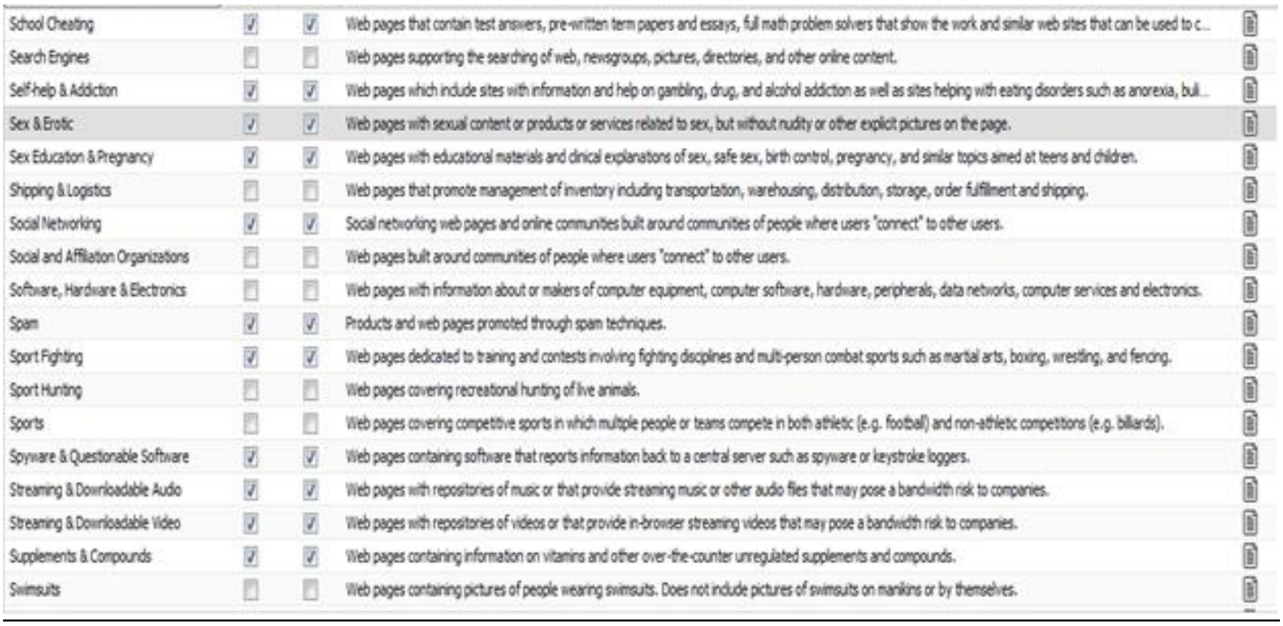
News	☐	☐	Web pages with general news information such as newspapers and magazines.	📄
No Content Found	☑	☑	Web pages which contain no discernable content which can be used for classification purposes.	📄
Non-traditional Religion & Occult	☐	☐	Web pages for religions outside of the mainstream or not in the top ten religions practiced in the world. Also includes occult and supernatural, extraterrestrial, folk rel...	📄
Nudity	☑	☑	Web pages that display full or partial nudity with no sexual references or intent.	📄
Nutrition & Diet	☐	☐	Web pages on losing weight and eating healthy, diet plans, weight loss programs and food allergies.	📄
Online Ads	☑	☑	Companies, web pages, and sites responsible for hosting online advertisements including advertising graphics, banners, and pop-up content. Also includes web page...	📄
Online Financial Tools & Quotes	☐	☐	Web pages for investment quotes, online portfolio tracking, financial calculation tools such as mortgage calculators, online tax preparation software, online bill paym...	📄
Online Information Management	☐	☐	Web pages devoted to online personal information managers such as web applications that manage to-do lists, calendars, address books, etc.	📄
Online Shopping	☐	☐	Websites and web pages that provide a means to purchase online.	📄
Online Stock Trading	☑	☑	Investment brokerage web pages that allow online trading of stocks, mutual funds and other securities.	📄
Parked	☑	☑	Web pages that have been purchased to reserve the name but do not have any real content.	📄
Parks, Rec Facilities & Gyms	☐	☐	Web pages which include parks and other areas designated for recreational activities such as swimming, skateboarding, rock climbing, as well as for non-professional ...	📄
Pay To Surf	☑	☑	Web sites that offer cash to users who install their software which displays ads and tracks browsing habits effectively allowing users to be paid while surfing the web.	📄
Peer-to-Peer	☑	☑	Web pages that provide peer-to-peer (P2P) file sharing software.	📄
Personal Pages & Blogs	☐	☐	Web pages including blogs, or a format for individuals to share news, opinions, and information about themselves. Also includes personal web pages about an individ...	📄
Personal Storage	☑	☑	Web sites used for remote storage of files, sharing of large files, and remote Internet backups.	📄
Pets & Animals	☐	☐	Web pages with information or products and services for pets and other animals including birds, fish, and insects.	📄
Pharmacy	☑	☑	Web pages which include prescribed medications and information about approved drugs and their medical use.	📄



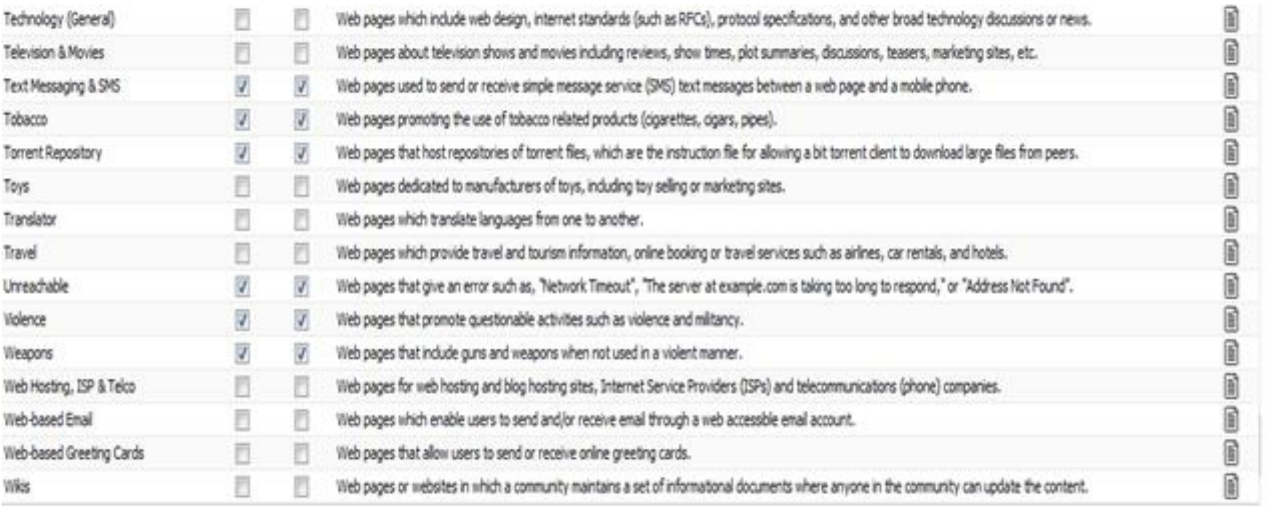
Philanthropic Organizations	☐	☐	Web pages with information regarding charities and other non-profit philanthropic organizations and foundations dedicated to altruistic activities.	📄
Phishing/Fraud	☑	☑	Manipulated web pages and emails used for fraudulent purposes, also known as phishing.	📄
Photo Sharing	☑	☑	Web pages that host digital photographs or allow users to upload, search, and exchange photos and images online.	📄
Physical Security	☐	☐	Web pages devoted to businesses and services related to security products or other security aspects excluding computer security.	📄
Piracy & Copyright Theft	☐	☐	Web pages that provide access to illegally obtained files such as pirated software (aka warez), pirated movies, pirated music, etc.	📄
Pornography	☑	☑	Web pages which contain images or videos depicting sexual acts, sexual arousal, or explicit nude imagery intended to be sexual in nature.	📄
Portal Sites	☐	☐	General web pages with customized personal portals, including white/yellow pages.	📄
Private IP Address	☑	☑	Web pages for Private IP addresses are those reserved for use internally in corporations or homes.	📄
Product Reviews & Price Comparisons	☐	☐	Web pages dedicated to helping consumers comparison shop or choose products or stores, but don't offer online purchasing options.	📄
Profanity	☑	☑	Web pages that use either frequent profanity or serious profanity.	📄
Professional Networking	☑	☑	Social networking web pages intended for professionals and business relationship building.	📄
R-Rated	☑	☑	Web pages whose primary purpose and majority of content is child appropriate, but who have regular or irregular sections of the site with sexually themed, non-edu...	📄
Real Estate	☐	☐	Web pages possessing information about renting, purchasing, selling or financing real estate including homes, apartments, office space, etc.	📄
Redirect	☑	☑	Web pages that redirect to other pages on other web sites.	📄
Reference Materials & Maps	☐	☐	Web pages which contain reference materials and are specific to data compilations and reference shelf material such as atlases, dictionaries, encyclopedias, census ...	📄
Religions	☐	☐	Web pages which cover main-stream popular religions world-wide as well as general religion topics and theology.	📄
Remote Access	☑	☑	Web pages that provide remote access to private computers or networks, internal network file shares, and internal web applications.	📄
Retirement Homes & Assisted Living	☐	☐	Web pages containing information on retirement homes and communities including nursing care and hospice care.	📄



Philanthropic Organizations	☐	☐	Web pages with information regarding charities and other non-profit philanthropic organizations and foundations dedicated to altruistic activities.
Phishing/Fraud	☑	☑	Manipulated web pages and emails used for fraudulent purposes, also known as phishing.
Photo Sharing	☑	☑	Web pages that host digital photographs or allow users to upload, search, and exchange photos and images online.
Physical Security	☐	☐	Web pages devoted to businesses and services related to security products or other security aspects excluding computer security.
Piracy & Copyright Theft	☐	☐	Web pages that provide access to illegally obtained files such as pirated software (aka warez), pirated movies, pirated music, etc.
Pornography	☑	☑	Web pages which contain images or videos depicting sexual acts, sexual arousal, or explicit nude imagery intended to be sexual in nature.
Portal Sites	☐	☐	General web pages with customized personal portals, including white/yellow pages.
Private IP Address	☑	☑	Web pages for Private IP addresses are those reserved for use internally in corporations or homes.
Product Reviews & Price Comparisons	☐	☐	Web pages dedicated to helping consumers comparison shop or choose products or stores, but don't offer online purchasing options.
Profanity	☑	☑	Web pages that use either frequent profanity or serious profanity.
Professional Networking	☑	☑	Social networking web pages intended for professionals and business relationship building.
R-Rated	☑	☑	Web pages whose primary purpose and majority of content is child appropriate, but who have regular or irregular sections of the site with sexually themed, non-edu...
Real Estate	☐	☐	Web pages possessing information about renting, purchasing, selling or financing real estate including homes, apartments, office space, etc.
Redirect	☑	☑	Web pages that redirect to other pages on other web sites.
Reference Materials & Maps	☐	☐	Web pages which contain reference materials and are specific to data compilations and reference shelf material such as atlases, dictionaries, encyclopedias, census ...
Religions	☐	☐	Web pages which cover main-stream popular religions world-wide as well as general religion topics and theology.
Remote Access	☑	☑	Web pages that provide remote access to private computers or networks, internal network file shares, and internal web applications.
Retirement Homes & Assisted Living	☐	☐	Web pages containing information on retirement homes and communities including nursing care and hospice care.



School Cheating	☑	☑	Web pages that contain test answers, pre-written term papers and essays, full math problem solvers that show the work and similar web sites that can be used to c...
Search Engines	☐	☐	Web pages supporting the searching of web, newsgroups, pictures, directories, and other online content.
Self-help & Addiction	☑	☑	Web pages which include sites with information and help on gambling, drug, and alcohol addiction as well as sites helping with eating disorders such as anorexia, buli...
Sex & Erotic	☑	☑	Web pages with sexual content or products or services related to sex, but without nudity or other explicit pictures on the page.
Sex Education & Pregnancy	☑	☑	Web pages with educational materials and clinical explanations of sex, safe sex, birth control, pregnancy, and similar topics aimed at teens and children.
Shipping & Logistics	☐	☐	Web pages that promote management of inventory including transportation, warehousing, distribution, storage, order fulfillment and shipping.
Social Networking	☑	☑	Social networking web pages and online communities built around communities of people where users "connect" to other users.
Social and Affiliation Organizations	☐	☐	Web pages built around communities of people where users "connect" to other users.
Software, Hardware & Electronics	☐	☐	Web pages with information about or makers of computer equipment, computer software, hardware, peripherals, data networks, computer services and electronics.
Spam	☑	☑	Products and web pages promoted through spam techniques.
Sport Fighting	☑	☑	Web pages dedicated to training and contests involving fighting disciplines and multi-person combat sports such as martial arts, boxing, wrestling, and fencing.
Sport Hunting	☐	☐	Web pages covering recreational hunting of live animals.
Sports	☐	☐	Web pages covering competitive sports in which multiple people or teams compete in both athletic (e.g. football) and non-athletic competitions (e.g. billiards).
Spyware & Questionable Software	☑	☑	Web pages containing software that reports information back to a central server such as spyware or keystroke loggers.
Streaming & Downloadable Audio	☑	☑	Web pages with repositories of music or that provide streaming music or other audio files that may pose a bandwidth risk to companies.
Streaming & Downloadable Video	☑	☑	Web pages with repositories of videos or that provide in-browser streaming videos that may pose a bandwidth risk to companies.
Supplements & Compounds	☑	☑	Web pages containing information on vitamins and other over-the-counter unregulated supplements and compounds.
Swimsuits	☐	☐	Web pages containing pictures of people wearing swimsuits. Does not include pictures of swimsuits on manikins or by themselves.



Technology (General)	□	□	Web pages which include web design, internet standards (such as RFCs), protocol specifications, and other broad technology discussions or news.	📄
Television & Movies	□	□	Web pages about television shows and movies including reviews, show times, plot summaries, discussions, teasers, marketing sites, etc.	📄
Text Messaging & SMS	☑	☑	Web pages used to send or receive simple message service (SMS) text messages between a web page and a mobile phone.	📄
Tobacco	☑	☑	Web pages promoting the use of tobacco related products (cigarettes, cigars, pipes).	📄
Torrent Repository	☑	☑	Web pages that host repositories of torrent files, which are the instruction file for allowing a bit torrent client to download large files from peers.	📄
Toys	□	□	Web pages dedicated to manufacturers of toys, including toy selling or marketing sites.	📄
Translator	□	□	Web pages which translate languages from one to another.	📄
Travel	□	□	Web pages which provide travel and tourism information, online booking or travel services such as airlines, car rentals, and hotels.	📄
Unreachable	☑	☑	Web pages that give an error such as, "Network Timeout", "The server at example.com is taking too long to respond," or "Address Not Found".	📄
Violence	☑	☑	Web pages that promote questionable activities such as violence and militancy.	📄
Weapons	☑	☑	Web pages that include guns and weapons when not used in a violent manner.	📄
Web Hosting, ISP & Telco	□	□	Web pages for web hosting and blog hosting sites, Internet Service Providers (ISPs) and telecommunications (phone) companies.	📄
Web-based Email	□	□	Web pages which enable users to send and/or receive email through a web accessible email account.	📄
Web-based Greeting Cards	□	□	Web pages that allow users to send or receive online greeting cards.	📄
Wikis	□	□	Web pages or websites in which a community maintains a set of informational documents where anyone in the community can update the content.	📄

Appendix 12

School Monitoring System

No monitoring can guarantee to be 100% effective we will ensure that our monitoring system is as robust as possible. It includes filtering for Key words, controlled by Google managed by Cyber Support, which automatically forces Safe Search and blocks access to inappropriate websites.

Our monitoring system covers the following content:

Content	Content or communications that:
Illegal	Is illegal (e.g. Child abuse images and terrorist content)
Bullying	Involves the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others.
Child Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity.
Drugs / Substance abuse	Displays or promotes the illegal use of drugs or substances.
Extremism	Displays sexual acts or explicit images.
Self- Harm	Promotes or displays deliberate self-harm.
Violence	Displays or promotes the use of physical force intended to hurt or kill.
Suicide	Suggest the user is considering suicide.
Commerce	Online pay for games and gambling.

A list of web filtering categories are in Appendix 1

We will ensure that our monitoring strategy meets the following principles:

Content	
Age appropriate	Includes the ability to implement variable monitoring appropriate to age. This will in turn define which alerts are prioritised and responded to.
Data retention	User accounts are disabled once pupils have left the school
Monitoring Policy (E-mail, E-Safety and Internet Policy)	Pupils are routinely reminded that their online access is monitored. They are taught about on-line safety

	and to behave appropriately and responsibly.
Impact	Cyber Support review regularly and monitor the impact of the systems. Weekly E-mails are sent to the school. Serious breaches are notified immediately.
Prioritisation (How alerts are generated and prioritised to enable rapid response)	Cyber Support send an automated E-Mail alerting web traffic events that violate our policy. They would inform us immediately if there was a serious breach e.g. multiple attempts to access an inappropriate website by a single user.
Reporting	Weekly E-Mail to Pauline Reid (School Business Manager)Dave Rooney (Principal), Raman Herr (ICT Lead).

Schools in England (and Wales) are required “to ensure children are safe from Terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering (Prevent Duty 2015.)
We ensure that access to illegal content is blocked, specifically that the filtering providers are IWF members and block access to illegal Child Abuse Images and Content (CAIC). Untangle.com are the manufacturer of our firewall/web filter. The filter automatically receives updates from a company called Zvelo who are members of the IWF. T**his company integrate the police assessed list of unlawful terrorist content, produced on behalf of the Home Office**.

Recognising that no filter can guarantee to be 100% effective, our filtering system manages the following content (and web search):

Content	Content that:
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.
Drugs / Substance abuse	Displays or promotes the illegal use of drugs or substances.
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance.
Malware / Hacking	Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content.
Pornography	Displays sexual acts or explicit images.
Piracy and copyright theft	Includes illegal provision of copyrighted material.
Self-Harm	Promotes or displays deliberate self- harm (including suicide and eating disorders).
Violence	Displays or promotes the use of physical force intended to hurt or kill.

We ensure that our system does not over block access so it does no lead to unreasonable restrictions and that our filtering system meets the following principles:

- Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role; Student and staff are differentiated.
- Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content; IT provider and onsite IT coordinator (R. Herr) have access to filtering controls.
- Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking.
- Identification - the filtering system should have the ability to identify users; filter is user and device aware (where possible)
- Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies. Encrypted traffic sent by apps like WhatsApp cannot be intercepted by the filter, school provided device should/are not permitted to use apps of this nature.
- **Multiple language support – the ability for the system to manage relevant languages.**
- Network level - filtering should be applied at 'network level' i.e., not reliant on any software on user devices. Untangle.com works at the network level (Untangle.com are the Filter Manufacturer)
- Reporting mechanism – the ability to report inappropriate content for access or blocking. Cyber Support send an automated weekly E- Mail to P Reid (School Business Manager, SDP, Prevent Trainer), D Rooney (Principal) and Raman Herr alerting the Academy to web traffic events that violate our policy. (E-mails provided by Microsoft and managed by Cyber Support). See Prevent Risk Assessment Appendix 3

  Cyber Support would inform us immediately if there was a serious breach e.g. multiple attempts to access an inappropriate website by a single user.
- Reports – the system offers clear historical information on the websites visited by your users; Data is retained for 30 days.

Lowbrook Academy

Appendix 13

Social Media Policy and Procedures

Objectives

Social media (e.g. Facebook, Twitter, Instagram, WhatsApp, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as YouTube have social media elements to them.

The Academy recognises the numerous benefits and opportunities which a social media presence offers. New technologies are an integral part of our lives and are powerful tools which open up teaching and learning opportunities for the Academy's staff in many ways. Staff, Governors, parents/carers and pupils are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children. It also compliant with 2018 GDPR legislation and practice.

This policy is intended to help members of the Academy's community to make appropriate decisions about the use of all forms of social media such as blogs, wikis, social networking websites, podcasts, forums, message boards, or comments on web-articles, such as Twitter, Facebook, LinkedIn and any other social media websites.

This document therefore sets out Lowbrook Academy's policy on social networking and aims to:

- Assist the Academy's staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice;

- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use;

- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken;

- Support safer working practice;

- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils;

- Reduce the incidence of positions of trust being abused or misused.

- Ensures that use is fully compliant with 2018 GDPR legislation.

Scope

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the Academy. This includes all members of the Academy's community (including employees, Governors, consultants, contractors, volunteers, casual workers, pupils, parents/carers, visitors and agency workers) who have access to and are users of the Academy's equipment. It does not form part of employee's contract of employment;

- Applies to such online communications posted at any time and from anywhere;

- Encourages the safe and responsible use of social media through training and education;

- Defines the monitoring of public social media activity pertaining to the Academy.

- Applies to all parents, guardians, visitors and volunteers engaging with Social Media with reference to all activities pertinent to this Academy.

The Academy respects privacy and understands that staff and pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the Academy's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on an Academy account or using the Academy's name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the Academy or impacts on the Academy, it must be made clear that the member of staff is not communicating on behalf of the Academy with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with pupils are also considered. Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

Organisational control

Roles & Responsibilities

- SLT
    - Facilitating training and guidance on Social Media use.
    - Developing and implementing and regularly reviewing this Social Media policy.
    - Taking a lead role in investigating any reported incidents.
    - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
    - Approval of Social Media account creation.
    - Create the account following SLT approval.
    - ***N.B.*** All Social Media accounts must be approved by the Principal in advance of any educational work being undertaken.
- Administrator/Moderator
    - Store account details, including passwords securely.
    - Be involved in monitoring and contributing to the account.
    - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring).
- Staff
    - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies.
    - Attending appropriate training.
    - Regularly monitoring, updating and managing content he/she has posted via school accounts.
    - Adding an appropriate disclaimer to personal accounts if/when naming the school.

Process for creating new accounts

The Academy's community is encouraged to consider if a social media account will help them in their work, e.g. a school Twitter account, or a Facebook page. Anyone wishing to create such an account must present a business case to the Principal which covers the following points:-

- The aim of the account;
- The intended audience;
- How the account will be promoted;
- Who will run the account (at least two staff members should be named);
- Will the account be open or private/closed.

Following consideration by the Principal and SLT, an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

The Academy's social media accounts must be monitored regularly and frequently (including during holidays). Parents/carers and pupils are not to use these accounts as a form of communication with the Academy and any queries or complaints must be directed via the school office in the standard way.

Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account. Mr Rooney is responsible for monitoring the schools platforms.

Behaviour

- The Academy requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies and the staff and Governors codes of conduct.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must make clear who they are in social media posts or accounts (e.g. include class name on Twitter posts). Anonymous posts are discouraged in relation to school activity. If it is not specified then it must be assumed that the post is from a member of the SLT.

- If a media enquiry is received about posts made using social media staff must inform SLT and not respond directly.

- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the Academy and will be reported as soon as possible to the Principal and escalated where appropriate.

- The use of social media by staff while at work may be monitored, in line with school policies. The Academy permits reasonable and appropriate access to private social media sites during non-contact time. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

- The Academy will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the Academy will deal with the matter internally using its disciplinary procedures. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and will take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.

- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

- Users will be fully compliant with GDPR 2018 regulations and will operate within the schools policies within these platforms.

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity. Please refer these immediately to the Principal who is the Safeguarding Lead (one of his deputies in his absence).

- If a conversation turns and becomes offensive or unacceptable, users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken. This must then be reported to the Principal or SLT member for further action

- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported to the Principal using the agreed school protocols. The Principal will use school policies and the law where appropriate.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Twitter)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the school's GDPR and data processing, digital and video images polies. Prior to posting photos of pupils, staff should check the parental consented in the class register. If anyone asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts-personal phones are not to be used unless there are exceptional circumstances and it is authorised by the Principal or Assistant Headteacher.
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- Staff
  - Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
  - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
  - Staff or Governors should ensure they do not disclose any personal information about members of the academy community or disclose any information that is confidential to

the Academy, including any information obtained as a result of their employment or position and not yet in the public domain.

- Staff or Governors should not post anything or act in such a way as to bring damage to the academy or its reputation.
- Staff or Governors must not knowingly “follow”, ”friend” or engage in any way on Social Media with any minor who is, or was a pupil at the academy under the age of 23 unless that pupil is a member of their family, a relation or under their guardianship or are following the individual solely as a consequence of fulfilling their parental or guardian responsibilities.
- Staff or Governors should avoid making any social media communications that could damage the Academy’s interests or reputation, even indirectly ;
- Staff and Governors must not use social media to defame or disparage the Academy, our staff, pupils or any third party; to harass, bully or unlawfully discriminate against staff, pupils or third parties; to make false or misleading statements; or to impersonate staff, pupils or third parties;
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken;
- The Academy permits reasonable and appropriate access to private social media sites.

- Pupil/Students
  - The Academy’s curriculum should enable the pupils to be safe and responsible users of social media.
  - Pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school’s behaviour policy.
  - Pupils must not access/ use social network sites within the Academy unless supervised during Curriculum time by a class teacher, e.g. Minecraft.
  - Pupils should not knowingly “follow”, ”friend” or engage in any way on Social Media with any teacher or ex-teacher who worked at the Academy unless they are a member of their family, a relation or guardian.
  - Pupils must not post malicious or fictitious comments on social networking sites about any member of the Academy community.

- Parents/Carers
  - Parents/carers will be made aware of their responsibilities regarding their use of social networking. Methods of academy communication include the prospectus, the website, newsletters, letters and verbal discussion.
  - Parents/carers are not expected to post pictures of pupils other than their own children on social networking sites.
  - Parents/carers should make complaints through official Academy channels rather than posting them on social networking sites.
  - If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
  - The Academy has an active Internet Safety programme which supports the safe and positive use of the Internet. This includes information on the website.
  - Parents/carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.
  - Parents/carers should not post malicious or fictitious comments on social networking sites about any member of the academy community.
  - The school reserves the right to suspend/block and remove parents/guardians from platforms. This is the responsibility and decision of the Principal or delegated members of staff.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school does not generally respond to social media comments made by others but reserves the right to do so.

Lowbrook Academy asks and encourages Governors, employees, pupils and parents to report any damaging or negative comment about the academy or a member of the academy community on social media to a member of the Senior Leadership team. Reports of any praise or positive comment are also welcome.

Dealing with incidents of online bullying and abuse.

Lowbrook Academy staff and pupils need to work together to prevent online bullying and abuse through the use of Social Media and to tackle it whenever it occurs.

All pupils are encouraged to report incidences of online bullying and abuse; whether experienced personally or if they are aware that another pupil is experiencing online bullying.

The Academy has a duty to ensure that:

- teachers have sufficient knowledge to deal with online bullying and abuse in the Academy. They will have a 'it could happy here' mindset and will refer to the Behaviour, Anti-bullying and Child Protection policies where required.
- the curriculum teaches pupils about the risks of new communications technologies, the consequences of their misuse, and how to use them safely
- all e-communications used on the Academy site or as part of school activities off-site are monitored
- Internet blocking technologies are continually updated and harmful sites blocked
- It works with pupils and parents/carers to make sure new communications technologies are used safely, taking account of local and national guidance and good practice
- security systems are in place to prevent images and information about pupils and staff being accessed improperly from outside the Academy .

The staff have a responsibility to:

- teach children safe Internet etiquette
- Ensure children are safe from Terrorist and extremist material when accessing the internet in school, including establishing appropriate levels of filtering (Prevent Duty 2015).
- apply the Academy's policy in monitoring electronic messages and images
- give pupils key guidance on:
    - personal privacy rights
    - material posted on any electronic platform
    - photographic images
    - take action if a pupil is being online bullied or is bullying someone else

- teach pupils the value of e-communications and the risks and consequences of improper use, including the legal implications.

Appendix 14

Staff Guide to managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Have a full and clear understanding of the schools GDPR policy and implement it accordingly.
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Lowbrook
Academy

Appendix 15

Template Parent Letter regarding Social Media

Dear Parents/Carers,

Social media is here to stay. The continuing popularity of platforms like Facebook and Twitter have prompted staff and governors to reflect on how we can all set a good example to the children in our school when using these, and other, social media tools.

We would like to invite all parents and carers from the Lowbrook Academy community to do the same.

I have attached an etiquette document to this letter that tells you what staff and governors have agreed and what our promises to the children, parents and carers are when using social networking sites. We hope that you will take up our invitation.

Thank you for your continued support.

Yours faithfully,

Dave Rooney
Principal

Appendix 16

Governors, Staff and Parents of Lowbrook Academy Best Practice on Social Networking Sites

The leadership, staff and governors have agreed an approach to the use of social networking sites that include the principles below. We are now inviting parents to join us in setting a good example for our children.

All parents are asked to join staff in setting a good example for our children by:

- Demonstrating courtesy and respect for staff, other parents and pupils when comments are placed on social networking sites.
- Using appropriate language when discussing school.
- Addressing any issues or concerns regarding school directly with the Head of School, a member of staff or governors.

All parents are asked to join staff in setting a good example for our children by **not**:

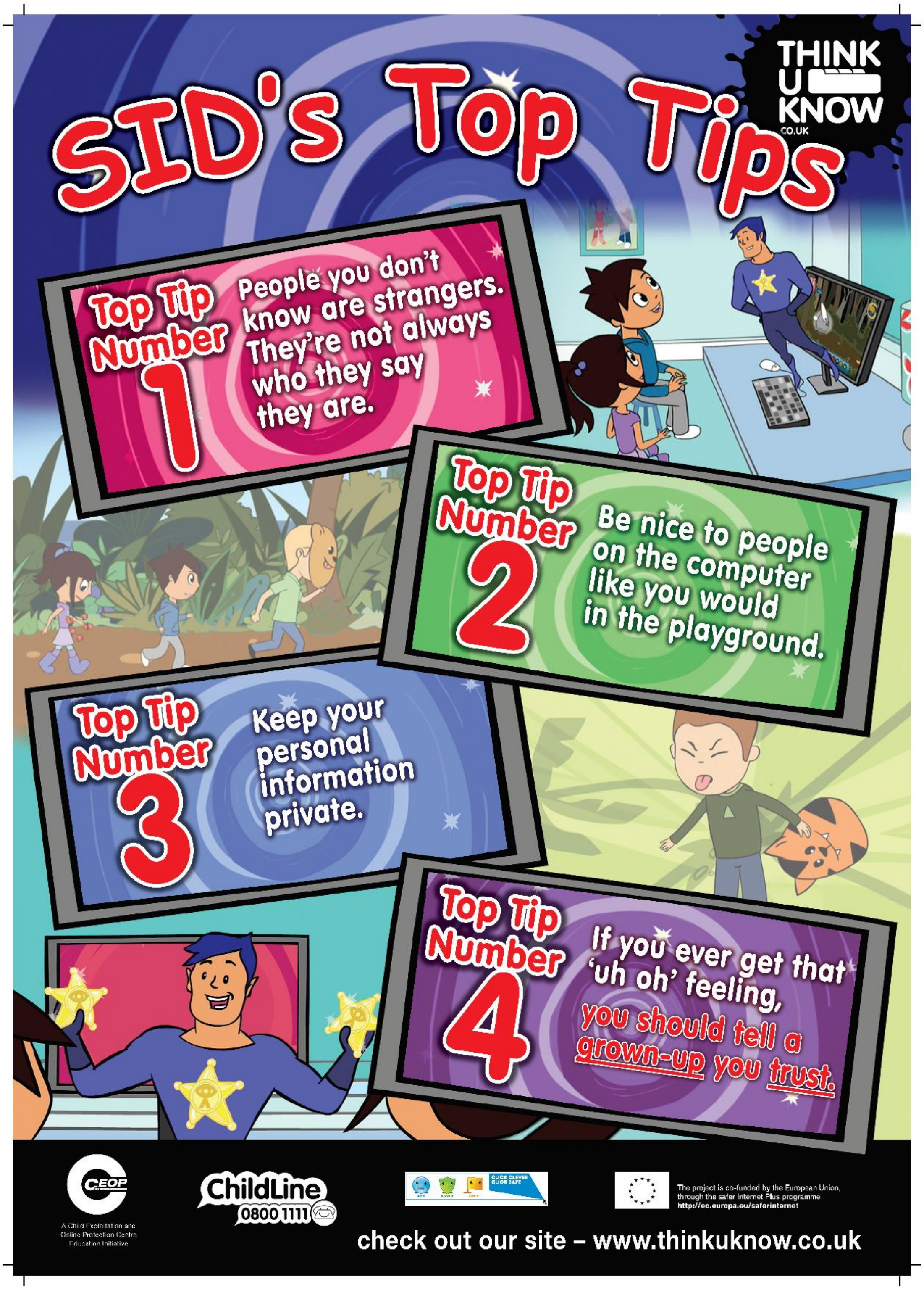
- Using social network sites to make derogatory comments or posting photographs which could bring staff into disrepute, including such comments about pupils, parents, other staff members, the senior leadership team, governors, local authority, school policy or the wider community.
- Posting photographs of other people's children on social network sites without their permission.

Our promise to the school community is:

- We will meet with you and use the Governing Body's policies and procedures to resolve concerns.
- We will work hard to resolve any concerns in the best interest of the whole community.
- We will act in the best interest of the whole community and honour our duty of care to our children.
- We will never conduct school business through social networking sites.

The school reserves the right to remove comments in violation of these principles or – in certain circumstances – to block users from our social media feeds.

Appendix 17



SID's Top Tips

THINK U KNOW .CO.UK

Top Tip Number 1 People you don't know are strangers. They're not always who they say they are.

Top Tip Number 2 Be nice to people on the computer like you would in the playground.

Top Tip Number 3 Keep your personal information private.

Top Tip Number 4 If you ever get that 'uh oh' feeling, you should tell a grown-up you trust.

CEOP
A Child Exploitation and Online Protection Centre Education Initiative

ChildLine 0800 1111

CLICK CLEVER CLICK SAFE

The project is co-funded by the European Union, through the safer Internet Plus programme http://ec.europa.eu/saferinternet

check out our site – www.thinkuknow.co.uk