Barker's Lane Community School

Online Safety Policy

This policy has been adapted from the SWGfl model policy from Hwb and applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Barker's Lane Community School to safeguard members of our school community online in accordance with principles of open government and with the law. Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.

This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Barker's Lane Community 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 online safety behaviour that take place out of school.

Policy development, monitoring and review

This Online Safety Policy has been developed by the governing body *of* Barker's Lane Community School made up of:

- *Headteacher*
- *Staff*
- *LA and Community governors*
- *Parent Governors*

Consultation with the whole school community has taken place previously through surveys and the school website.

Schedule for development, monitoring and review

This Online Safety Policy was approved by the *school governing body on:*	
Signed:	*Chair of Governors*
The implementation of this Online Safety Policy will be monitored by:	*SLT* *Community and H&S Sub-Committee*
Monitoring will take place at regular intervals:	*Annually*
The *governing body* will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Termly through the HT Report to GB*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*Autumn 2022*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*Simon Billington – ICT Strategy Manager (LA)* *John Hodgson – Education Social Work Manager (LA)*

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- *logs of reported incidents*
- *surveys/questionnaires of:*
    - *learners*
    - *parents and carers*
    - *staff.*

Policy and leadership

Responsibilities

In order to ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns and misuse as soon as these become apparent.

Headteacher

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding.
- The headteacher and deputy headteacher are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher is responsible for ensuring that relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the Welsh Government and UKCIS document Five key questions for governing bodies to help challenge their school to effectively safeguard their learners. This will be carried out by the Community and H&S Committee whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- reporting to relevant *governors group/meeting*

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Online Safety Lead

Mrs Edwards, headteacher is the named person responsible for safeguarding and is the online safety lead.

The online safety lead will:

- work closely on a day-to-day basis with the Designated Safeguarding Person (DSP), where these roles are not combined
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education across the school and beyond
- liaise with teachers to ensure that the online safety curriculum is planned and embedded
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- identify sources of training and advice for staff/governors/parents/carers/learners
- liaise with LA technical staff, pastoral staff and support staff
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents
- attend relevant governing body meetings
- liaises with the local authority/relevant body.

Designated Safeguarding Person (DSP)

Mrs Edwards, headteacher is the designated safeguarding person (DSP).

The Designated Safeguarding Person is trained in online safety issues and is aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying.

AoLE Groups

Teachers will work to develop a planned and coordinated online safety education programme. This will be provided through:

- a discrete programme
- the Digital Competence Framework
- personal and social education/sex and relationships education
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to the headteacher for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned learners 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 lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the Live-streaming and video-conferencing: safeguarding principles and practice guidance
- they have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Network manager/technical staff

The Local Authority is the managed technical service provider.

The local authority is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy in order to carry out their work effectively in line with school policy
- the *school* technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the local authority or other relevant body
- users may only access the networks and devices through a properly enforced password protection policy
- they keep up-to-date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- the use of the technical and communications systems is regularly monitored in order that any misuse/attempted misuse can be reported to the headteacher for investigation and action
- *the filtering policy), is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person* (see appendix 'Technical Security Policy template' for good practice).

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- should avoid plagiarism and uphold copyright regulations
- will be expected to know and follow school Online Safety Policy
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Parents and 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 and carers understand these issues through:

- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc

Parents and carers will be encouraged to support the school in:

- *reinforcing the online safety messages provided to learners in school*
- *the use of their children's personal devices in the school (where this is allowed)*
- *appropriate use of digital and video images taken at school events*
- *access to parents' sections of the website / social media pages*

Professional Standards

There is an expectation that national professional standards will be applied to online safety as in other aspects of school life i.e.

- there is a consistent emphasis on the central importance of literacy, numeracy and digital competence. Learners will be supported in gaining skills across all areas of learning and every opportunity will be taken to extend learners' skills and competence
- there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience.
- practitioners are able to reflect on their practice, individually and collectively, against nationally agreed standards of effective practice and affirm and celebrate their successes
- policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Policy

Online Safety Policy

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they can use digital technologies responsibly, protecting themselves and the school and how they can use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels on the shared staff drive
- is published on the school website.

Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

The Online Safety Policy and appendices define acceptable use at the school. Within the appendices there are acceptable use agreements for:

- learners – differentiated by age. Learners will be introduced to the acceptable use rules at induction, the start of each school year and regularly re-enforced during lessons, assemblies and by posters around the school.
- staff /volunteer AUAs will be agreed and signed by staff and volunteers
- parent/carer AUAs inform them of the expectations of acceptable use for their children and seek permissions for digital images, the use of cloud systems etc.

The acceptable use agreements will be communicated/re-enforced through: (amend as appropriate)

- staff induction and handbook
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website

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 N.B. Schools should refer to guidance about dealing with nudes and semi-nudes being shared.					X
	grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003					X
	possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character), contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	promotion of extremism or terrorism				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	
Activities that might be classed as cyber-crime under the Computer Misuse Act (1990):						X

• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – further information here					
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	
Online gaming (educational)		x			
Online gaming (non educational)				x	
Online gambling				x	
Online shopping/commerce		x			
File sharing	x				
Use of social media			x		
Use of messaging apps			x		
Use of video broadcasting, e.g. YouTube		x			

	Staff and other adults							
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
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 e-mail addresses in school, or on school network								
Use of school e-mail for personal e-mails								
Use of messaging apps								
Use of social media								
Use of blogs								

**Personal calls / texts are permitted in some circumstances e.g emergency; waiting on doctor's advice, in these cases staff inform a member of the SLT*

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

- the official school e-mail service may be regarded as safe and secure and is monitored. Users should be aware that e-mail communications are monitored. *Staff and learners should therefore use only the Hwb e-mail service to communicate with others when in school, or on school systems (e.g. by remote access)*
- users must immediately report to the nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- any digital communication between staff and learners or parents/carers (e-mail, chat, learning platform, etc.) must be professional in tone and content. *These communications may only take place on official (monitored) school systems. Personal e-mail addresses, text messaging or social media must not be used for these communications*
- *learners should be taught about online 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 digital citizenship and the need to communicate appropriately when using digital technologies.*
- *personal information should not be posted on the school website and only official e-mail addresses should be used to identify members of staff.*

Reporting and responding

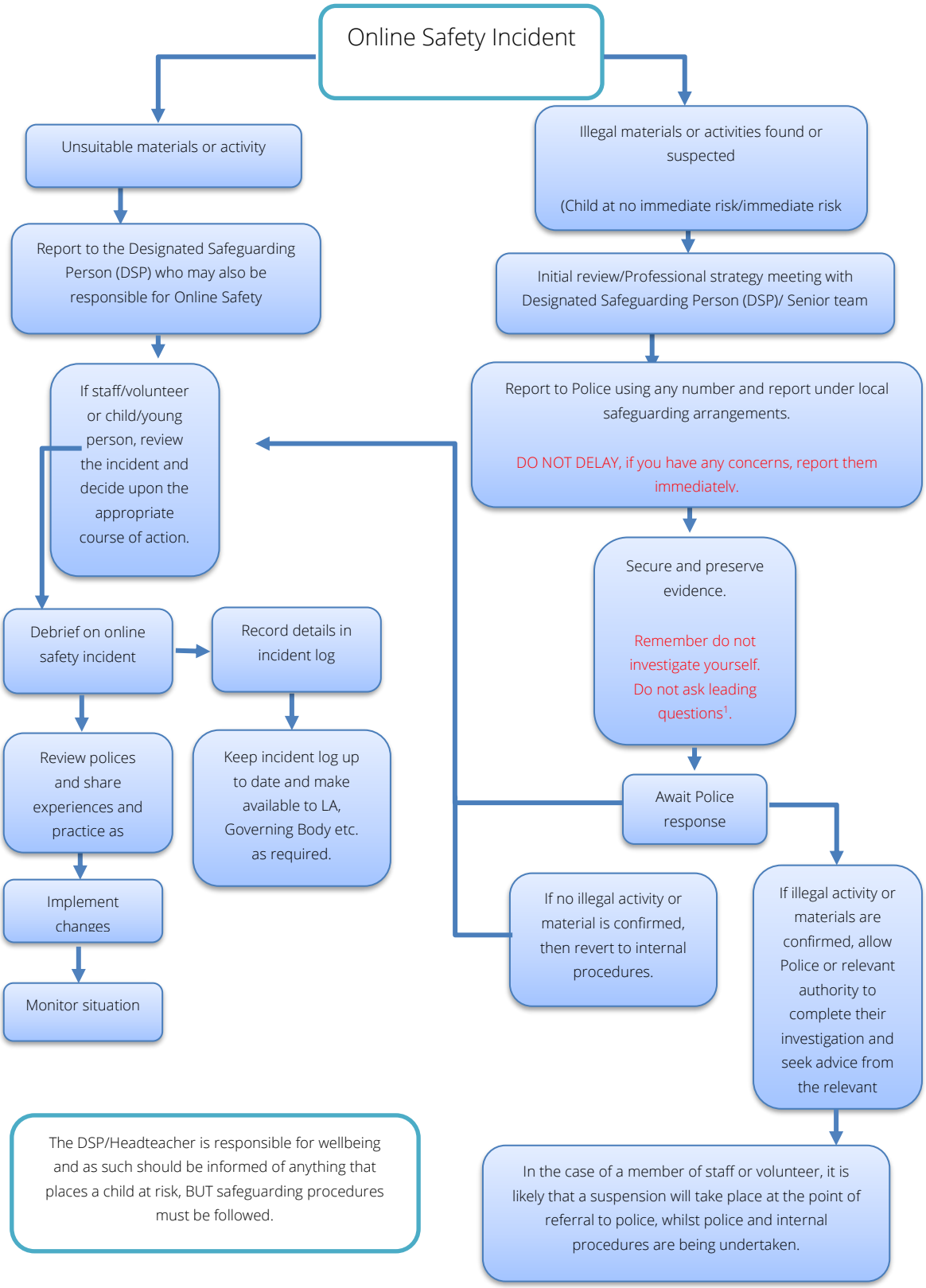
The school will take all reasonable precautions to ensure online safety for all school users, but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and grievance policies.
- all members of the school community will be made aware of the need to immediately report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Person and other responsible staff have appropriate skills and training to deal with the various risks related to online safety
- if there is any suspicion that the incident involves child abuse images, any other illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the normal school safeguarding procedures and the police informed. In these circumstances any device involved should be isolated to support a potential police investigation. In addition to child abuse images such incidents 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
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials.
- any concern about staff misuse will be reported immediately to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- as long as there is no suspected illegal activity devices may be checked using the following procedures:
    - one or more senior members of staff should be 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 learners and if necessary can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). 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 above).
    - 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 (as relevant)
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g. peer support for those reporting or affected by an online safety incident
- incidents should be logged on My Concern
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP; Keeping safe online on Hwb
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - *teachers for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
    - *staff, through regular briefings*

- *learners, through assemblies/lessons*
- *parents/carers, through newsletters, school social media, website*
- *governors, through regular safeguarding updates*
- *local authority/external agencies, as relevant*

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.


Online Safety Incident
Unsuitable materials or activity
Report to the Designated Safeguarding Person (DSP) who may also be responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as
Keep incident log up to date and make available to LA, Governing Body etc. as required.
Implement changes
Monitor situation
Illegal materials or activities found or suspected
(Child at no immediate risk/immediate risk
Initial review/Professional strategy meeting with Designated Safeguarding Person (DSP)/ Senior team
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediatelv.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
The DSP/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

School actions

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

Learner actions

Incidents	Refer to class teacher/tutor	Refer to Head of Department/Head of Year/other	Refer to Headteacher/Principal	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet	Issue a warning	Further sanction, e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons.	x								
Unauthorised use of mobile phone/digital camera/other mobile device.		x	x						
Unauthorised use of social media/messaging apps/personal e-mail.		x	x						
Unauthorised downloading or uploading of files.	X								
Allowing others to access school network by sharing username and passwords.	X								
Attempting to access or accessing the school network, using another learners' account.	x	x	x						
Attempting to access or accessing the school network, using the account of a member of staff.			X			x		X	
Corrupting or destroying the data of other users.			X			x	x	x	
Sending an e-mail, 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 or 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	
Accidentally accessing offensive or pornographic material and failing to report the incident.	x					X			
Deliberately accessing or trying to access offensive or pornographic material.			X			x	x	x	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.			x						

Staff Actions

Incidents	Refer to line manager	Refer to Headteacher/ Principal	Refer to local authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering, etc.	Issue a 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
Inappropriate personal use of the internet/social media/personal e-mail		x	x					
Unauthorised downloading or uploading of files.		x						
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.		x						

Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner		x	x					
Deliberate actions to breach data protection or network security rules.		x	x					X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x	x					X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.		x	x					X
Using personal e-mail/social networking/messaging to carrying out digital communications with learners and parents/carers		x	x					x
Actions which could compromise the staff member's professional standing		x						
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		x	x					
Using proxy sites or other means to subvert the school's filtering system.		x			x			
Accidentally accessing offensive or pornographic material and failing to report the incident.		x						
Deliberately accessing or trying to access offensive or pornographic material		x	x					x
Breaching copyright or licensing regulations.		x	x					
Continued infringements of the above, following previous warnings or sanctions.		x	x					x

Education

Online Safety Education Programme

While regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

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

- a planned online safety curriculum across all year groups and a range of subjects, (e.g. DCF/PSE/RSE/Health and Well-being) and topic areas and should be regularly revisited
- key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language. Learners considered to be at increased risk online (e.g. children in care, ALN learners, learners experiencing loss or trauma or mental health issues) are provided with targeted or differentiated online safety education
- learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. NB additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet
- *learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school*
- *staff should act as good role models in their use of digital technologies the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that learners 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 learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit*

- *it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other nominated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need*

Contribution of Learners

The school acknowledges, learns from and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- *mechanisms to canvass learner feedback and opinion e.g. questionnaires, class discussion.*
- *appointment of digital leaders*
- *learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns*
- *learners designing/updating acceptable use agreements*
- *contributing to online safety events with the wider school community.*

Staff/volunteers

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

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- *the Online Safety Lead and Designated Safeguarding Person (or other nominated person) will receive regular updates through attendance at external training events, (e.g. Hwb Keeping safe online training events, from the Regional Consortium/SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations*
- *this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days*
- *the Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.*

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in a number of ways such as:

- Hwb training – Online safety for governors
- attendance at training provided by the local authority or other relevant organisation (e.g. SWGfL)
- participation in school training/information sessions for staff or parents

Families

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

- *regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes*
- *regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / providing links to appropriate websites*
- *the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.*
- *letters, newsletters, website, learning platform, Hwb*
- *high profile events/campaigns e.g. Safe Internet Day*
- *reference to the relevant web sites/publications, e.g. Hwb Keeping safe online, www.saferinternet.org.uk/ www.childnet.com/parents-and-carers (see Appendix for further links/resources).*
- *sharing good practice with other schools in clusters and or the local authority*

Technology

The Local Authority act as Network Manager / Technical Staff as a managed service provider.

They are responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures are implemented by the Local Authority.

The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering

- the school filtering policies are agreed by the Local Authority and senior leaders and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours

- the LA manages access to content across its systems for all users. The filtering provided meets the standards defined by the Welsh Government.
- internet access is filtered for all users
- illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider.
- there are established and effective routes for users to report inappropriate content
- any requests for filtering changes are made to the Local Authority
- *younger learners will use child friendly/age appropriate search engines e.g. SWGfL Swiggle*
- there is an appropriate and balanced approach to providing access to online content according to role and/or need
- *where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.*

If necessary, the school will seek advice from, and report issues to the Local Authority.

Monitoring

The school protects users and school systems through:

- physical monitoring (adult supervision in the classroom)
- *liaison with the Local Authority if there is any issue with breach of the filter*

Users are made aware, through the acceptable use agreements, that monitoring takes place.

Technical Security

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements by the Local Authority. This includes:

- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of copies off-site or in the cloud by the Local Authority
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be reviewed by the headteacher
- all users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details. Sharing of passwords or ID and passwords could lead to an offence under the Computer Misuse Act 1990. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password
- the master account passwords for the school systems are kept in a secure place, e.g. SIMs.
- passwords are issued by the LA or Hwb

- records of learner usernames and passwords for Foundation Phase learners can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- password requirements for learners at Key Stage 2 and above should increase as learners progress through school
- the School Business Manager is responsible for ensuring that software licence logs are accurate and up-to-date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- any actual/potential technical incident/security breach should be reported to the headteacher or deputy headteacher
- appropriate security measures are in to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc., from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- an agreed policy is in place for the provision of temporary access of 'guests', (e.g. trainee teachers, supply teachers, visitors) onto the school systems
- an agreed policy is in place regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school
- staff should not download executable files / install programmes on school devices without seeking permission from the headteacher
- personal data should not be taken off the school site e.g. USB sticks, unless safely encrypted.

Mobile technologies

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

At Barker's Lane, the following is employed:

	School devices			Personal devices	
	School owned for individual use	School owned for multiple users	Authorised device[1]	Student owned	Staff owned
Allowed in school	Yes	Yes		At times with specific permission (Mobile phones are stored by school staff during the day)	Yes
Full network access	Yes	Yes		No	No
Internet only				No	At times with specific permission
No network access				No	No

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk
- guidance for learners, parents/carers

School staff should ensure that:

- no reference should be made in social media to learners, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community

- personal opinions should not be attributed to the school or local authority
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

When official school social media accounts are established there should be:

- a process for approval by senior leaders
- clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, 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
- 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 school permits reasonable and appropriate access to private social media sites*

Monitoring of public social media

- As part of active social media engagement, the school will pro-actively monitor the Internet for public postings about the school
- the school should effectively respond to social media comments made by others according to a defined policy or process
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

Digital and video images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- should a maintained school or setting choose to use live-streaming or video-conferencing, governing bodies, headteachers and staff must have full regard to national safeguarding guidance and local

safeguarding policies and should take note of the guidance contained in the Live-streaming and video-conferencing: safeguarding principles and practice guidance

- when using digital images, staff should inform and educate learners 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 *learners* 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, storage, distribution and publication of those images. Staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school equipment wherever possible. If the personal equipment of staff is used for such purposes, images should be deleted as soon as possible*
- *care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute*
- *learners must not take, use, share, publish or distribute images of others without their permission*
- *photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images*
- *learners' full names will not be used anywhere on a website or blog, particularly in association with photographs*
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored on the school network in line with the school retention policy
- *learners' work can only be published with the permission of the learner and parents/carers.*

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Seesaw
- Email

The school website is hosted by School Says. The school ensures that good practice has been observed in the use of online publishing e.g. use of digital and video images, copyright, identification of young people,

publication of school calendars and personal information – ensuring that there is no risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected and full names are not published.

The school public online publishing provides information about online safety e.g. publishing the schools Online Safety Policy; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. The school has a Data Protection policy in place.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g. online safety education, awareness and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendices:

Appendix 1: Hwb additional services consent form
Appendix 2: Hwb Rules and Acceptable Use Agreement
Appendix 3: Parent / Carer Acceptable Use Agreement
Appendix 4: Information Sharing Consent Form
Appendix 5: Staff (and Volunteer) Acceptable Use Policy Agreement
Appendix 6: Record of reviewing devices/internet sites
Appendix 7: Reporting Log

The Welsh Government and SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this school Online Safety Policy template and of the 360 safe Cymru online safety self-review tool:

Acknowledgements:

- Members of the SWGfL Online Safety Group
- Representatives of Welsh local authorities
- Representatives from a range of Welsh schools involved in consultation and pilot groups

Appendix 1: Hwb additional services consent form

The Hwb platform provides all maintained schools in Wales with access to a wide range of centrally-funded, bilingual digital tools and resources to support the digital transformation of classroom practices. The Hwb platform is managed and operated by the Welsh Government.

All learners in maintained schools in Wales must be provided with a secure log-in to the Hwb platform. This is because mandatory reading and numeracy tests, currently on paper, will be moving online and must be completed by each pupil via the platform. In order to provide your child with a secure log-in, the school will be sending basic information to the Welsh Government. The log-in will allow your child to take the mandatory online assessments, known as 'personalised assessments'.

For more information about the Hwb platform and how information about your child is used, please see https://hwb.gov.wales/privacy.

For more information about the online personalised assessments, please see http://learning.gov.wales/resources/collections/national-reading-and-numeracy-tests?lang=en#collection-2

Additional services

If you agree, Welsh Government can also provide your child with access, via the Hwb platform, to a variety of additional services which are provided by other organisations. These include online learning environments such as Hwb Classes, Microsoft Office 365, Google for Education, and other relevant educational tools and resources. Welsh Government is making these additional services available to help your child access educational resources. These additional services are centrally funded and there is no cost for you or for your school to access and use them.

Welsh Government will only provide access to these additional services if you sign the form below to indicate your agreement.

Your agreement

If you agree:

- we will tell Welsh Government to provide access to the additional services
- Welsh Government will share information about your child with its service providers, including Microsoft and Google Education, in order to enable access to the additional services.

If you do not agree, we will still share information about your child with Welsh Government to set up a secure log-in for the Hwb platform, but your child will not be able to access the additional services.

If you wish to withdraw your consent, please contact the head teacher within your child's school.

Parent / Carer Signature

Signed ..... Please sign and date this form if you agree to the above:

Name .....

Date ..... (signed)

..... (date)

Appendix 2: Hwb Rules and Acceptable Use Agreement

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

- Be polite - never post something online or send an email which is likely to cause offence to someone else. Don't upset or bully anyone.
- Be careful what you say and how you say it, use acceptable language at all times. What you do and say on Hwb is recorded and will be viewed by other people including your teacher.
- Be safe – don't reveal anything about yourself or about your friends (especially your address or phone numbers). This is very important.
- Be security smart - keep your username and password safe.
- Protect the school community by telling a teacher if you see anything that might cause upset or harm to yourself, other pupils or teachers in the school. Use the Worry Box if you want.
- Only link to other websites if you are sure they are safe to visit and are appropriate for your classmates and friends.
- When sending an email don't communicate with people you or your teachers don't know. Don't open emails if you don't know the sender. If you are unsure, always check with your teacher. Email use may be monitored.
- Do not create, store or send offensive or indecent images or other material. This is very serious and usually has to be reported to authorities.
- Don't upload anything to the platform that you can't share with your teacher.

Your school may have to look at taking you offline if you cannot follow these rules which are for the good of everyone, yourself included.

I agree with the Acceptable Use statements above and will use Hwb and other digital devices properly.

***Child's name …… Signed ……..…….. Date ……**

I **will support** my child to adhere to the agreement and safe use of internet including Hwb, additional services and other digital devices.

***Parental Signature:……. Date:……**

Appendix 3: Parent / Carer Acceptable Use Agreement

Child's Name: …… Parent / Carer's Name/s: ……

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

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

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

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

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

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in school, out of school on visits for example and in wraparound care. These images may then be used in presentations in subsequent lessons or for staff professional development. Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

The school will comply with the General Data Protection Regulation (GDPR) and will also ensure that when images are published outside of school that the young people can not be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the GDPR). **To respect privacy and in some cases protection, these images (where children other than your own are in a photograph) 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.**

Your Agreement (Please sign one of the statements below)

As the parent / carer of the above *pupil*, I agree to the school taking and using digital / video images of my child. I understand that the images will only be used to support learning activities, staff professional development or in publicity that reasonably celebrates success and promotes the work of the school or wraparound care.
I agree that if I take digital or video images at or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images. I will also support the school by communicating this message to other family members / friends who attend on behalf of myself e.g. grandparents / siblings / aunts and uncles, etc.

Signed …….. Date…….

As the parent / carer of the above *pupil*, I do not agree to the school taking and using digital / video images of my child. I understand that my child will not have their photograph taken in school for the purpose of learning and / or celebration and will be provided with alternative provision during public performance of concerts, sports day, etc.
I understand that by not choosing to abide by photography guidelines, I forfeit the opportunity to attend public performances, including concerts, sports day, etc.

Signed …….. Date…….

If you give consent and wish to withdraw this in future please contact the school office.

Appendix 4: Information Sharing Consent Form

We use a range of your / your child's personal data to fulfil our statutory duties for learning and wellbeing. Some of this information, for example personal details, contact information, medical information, educational attainment etc is essential and there is a legitimate and lawful basis for us to collect and share this.

For more information about how this information is collected and used, please see our Privacy Notice on the school website:

https://www.barkerslaneprimary.co.uk/wp-content/uploads/2018/05/Privacy-Notice-May-18.pdf

There are however other ways in which we use your child / your personal information to help us provide learning opportunities, celebrate these and provide information to parents / carers which require consent from yourselves under the new GDPR.

Barker's Lane School will only provide access to the following services if you sign the form overleaf to indicate your agreement.

No	What do we want to use the personal information for?	Why is this important?	What alternative will the school offer if I do not give consent?
1	Display Displaying your child's Christian name, initial of their surname and their photograph within school.	For celebrating your child's work on classroom / school displays. Putting names on coat pegs and trays so they are easily identifiable by your child. Names on workbooks and other classroom supports for learning and class management.	Work would be housed in books only. Pegs / trays would be labelled with picture of your child's choice. Your child's initials and a picture of their choice would be put on their workbooks and other supports.
2	Seesaw Your child's Christian name, initial of their surname (where necessary), photographs of your child and their individual and collaborative work to be saved and shared with yourself and other Barker's Lane	To share activities / learning regularly with parents. For teachers to record evidence of practical learning.	Workbooks are usually shared twice per year at Parents' Evening from Y2-6. Photographs / recordings with permission can be stored on the school server as evidence.

	children / families involved on Seesaw. **Please note Seesaw is an application from the USA, therefore is hosted outside of the UK.** **Seesaw Privacy Policy** https://web.seesaw.me/privacy/	For teachers to provide additional verbal feedback to your child which they can use to improve learning. To provide pre-learning opportunities / consolidation.	Written feedback can be provided, although proven to not be as effective as verbal feedback.
3	Home-School Communication Text messaging service and use of your email address to communicate information such as reminders, notifications, changes to arrangements, letters, newsletters through the Teachers to Parents – Eduspot website. **Supplier Privacy Policy** https://eduspot.co.uk/privacy-policy/	To keep parents up to date and provide efficient home-school communications. To ensure parents can be informed very quickly of an incident, for example those detailed in our evacuation or sheltering and lock down plan, etc.	Parents can register for the free school app if they wish to receive notifications or regularly check the school website for changes / information.

If you agree we will use your child's / your personal information for the purposes listed above.

We will share the personal information listed with service providers in order to enable access to the services.

Please select from the following three options, tick the box/es, sign and date.

Your agreement

☐ I give consent for all of the listed items 1-3.

Child's Name: …….

Signed…… Name…… Date……

If you do not agree with all of the items 1-3, we will still use the information that is legitimate and lawful to carry our statutory duties. However please tick the boxes which you do give consent for:

☐ 1. Display ☐ 2. Seesaw ☐3. Home-School Communication

Child's Name: …….

Signed…… Name…… Date……

If you do not agree with any of the items 1-3, we will still use the information that is legitimate and lawful to carry our statutory duties.

☐ I do not give consent for any of the items and understand the alternative that is offered for my child / family.

Child's Name: …….

Signed…… Name…… Date……

Appendix 5: Staff (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 access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- that school 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 technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities 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 systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the children and young people in my care in the safe use of digital technology and embed online safety in my work with children and young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, e-mail, etc.) out of school, and to the transfer of personal data (digital or paper based) out of the school
- I understand that the school digital 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.

I will be professional in my communications and actions when using school 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/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in the school in accordance with school policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

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

- If I use my personal mobile devices 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 if I use them to connect to school internet / network.
- I will not use personal e-mail addresses on the school ICT systems without seeking permission from the headteacher.
- I will not open any hyperlinks in e-mails or any attachments to e-mails, unless the source is known and trusted, or if I have any concerns about the validity of the e-mail (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, terrorist or extremist 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 and I have been given permission to do so.
- 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 Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner 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 digital technology equipment in the school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use 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 digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....

Signed: .....

Date: .....

Appendix 6: Record of reviewing devices/internet sites

(responding to incidents of misuse)

School: .....

Date: .....

Reason for investigation: .....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

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

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and action proposed or taken

Appendix 7: Reporting Log School: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Legislation

Schools should be aware of the legislative framework under which this Online 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 event of an online 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.

Schools may wish to view the National Crime Agency (NCA) website which includes information about "Cyber Choices: Helping you choose the right and legal path". The TARIAN Regional Cyber Crime Unit (RCCU) now has dedicated 'Cyber Prevent' officers whose role is to prevent young people from committing cybercrime and/or re-offending. Supportive resources are available on Hwb and there is a useful summary of the Computer Misuse Act on the NCA site.

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.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- facilitate the secure transfer of information within the European Union
- prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business
- give the public confidence about how businesses can use their personal information
- provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it
- give data subjects greater control over how data controllers handle their data
- place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data
- require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused
- require the data user or holder to register with the Information Commissioner's Office (ICO).

All data subjects have the right to:

- receive clear information about what you will use their data for
- access their own personal information
- request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan
- prevent or query about the automated processing of their personal data.

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 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

A 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 Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems

Serious Crime Act 2015

This Act introduced a new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE).

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison. For further guidance or support please contact the Revenge Porn Helpline

Links to other organisations or documents

The following links may help those who are developing or reviewing a school Online Safety Policy and creating their online safety provision:

Welsh Government

Safeguarding children (including Keeping Learners Safe and Respect and resilience: developing community cohesion)
School bullying advice

Hwb

Hwb homepage
Keeping safe online
Support Services
Hwb Support Centre
Enhancing digital resilience in education: An action plan to protect children and young people online - 2020
Online safety: Five key questions for governing bodies to help challenge their schools and colleges to effectively safeguard their learners
Digital Competence Framework
Health and Well-being AOLE
Keeping Learners Safe Modules 4 and 5 Online Safety for Practitioners and Governors
Live-streaming and video-conferencing: safeguarding principles and practice

UK Safer Internet Centre

UK Safer Internet Centre
South West Grid for Learning
Childnet
Professionals Online Safety Helpline
Internet Watch Foundation
Report Harmful Content
UK Safer Internet Centre – Research Summaries

Others

CEOP / ThinkUKnow
INSAFE/Better Internet for Kids
UK Council for Internet Safety (UKCIS)

Tools for Schools

SWGfL Test filtering

UKCIS Digital Resilience Framework

Bullying/Online-bullying/Sexting/Sexual Harassment

Childnet – Project deSHAME – Online Sexual Harassment

Data Protection

ICO Guides for Education (wide range of sector specific guides)

IRMS - Records Management Toolkit for Schools

ICO Guidance on taking photos in schools

Infrastructure/Technical Support

UKSIC – Appropriate Filtering and Monitoring

NCA Guide to the Computer Misuse Act

NEN Advice and Guidance Notes

SWGfL – Test Filtering

Working with parents and carers

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Internet Matters

Prevent

Prevent Duty Guidance

Prevent for schools – teaching resources

NCA – CyberChoices

TARIAN Regional Cyber Crime Unit (RCCU)

Hwb - TrustMe

Research

Ofcom –Media Literacy Research