Lyminster Primary School

E-Safety Policy

Lyminster Primary School Wick Street, Littlehampton, West Sussex, BN17 7JZ

Approved: March 2019
Review Date: February 2021

POLICY

Contents

E-Safety Policy

This policy sets out the ways in which the school will:

- Educate all members of the school community on their rights and responsibilities with the use of technology
- Build both an infrastructure and culture of e-safety
- Work to empower the school community to use the internet as an essential tool for life-long learning

This policy is used in conjunction with other school policies and has been developed in consultation with the Health & Safety Working Party.

Scope of the policy

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

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 such as cyber-bullying, which may take place out of school, but are linked to membership of the school.

The school will manage e-safety as described within this policy and associated positive behaviour and anti-bullying policies, and will inform parents and carers of known incidents of inappropriate e-safety behaviour that take place in and out of school.

Schedule for Development, Monitoring and Review

The implementation of the e-safety policy will be monitored by the Health & Safety Working Party meeting termly and reporting to the Governors annually.

The impact of the policy will be monitored by the Health & Safety Working Party by looking at:

- Log of reported incidents
- Internet monitoring log
- Surveys or questionnaires of learners, staff, parents and carers
- Other documents and resources
- Future developments

The e-safety policy will be reviewed annually or more regularly in the light of significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

Date adopted by the Governing Body: _____________

ROLES AND RESPONSIBILITIES

The Headteacher is responsible for ensuring the safety (including e-Safety) of all members of the school community, though the day to day responsibility for e-Safety can be delegated.

Headteacher is the appointed e-Safety Leader and in conjunction with the Designated Safeguarding Lead and will have an overview of the serious child protection issues to arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate on-line contact with adults, potential or actual incidents of grooming and cyber-bullying.

A Health & Safety Working Party will work with the e-Safety Leader or their delegated Senior Leadership representative to implement and monitor the e-Safety policy and AUPs (Acceptable User Policies) **(Appendix 1)**. This group is made up several members as per the Working Party terms of reference **(Appendix 2).** They meet on a termly basis.

Role	**Responsibility**
Governors	• Approve and review the effectiveness of the e-Safety Policy • Delegate a governor to act as e-Safety Link Governor • E-Safety Governor works with the e-Safety Leader to carry out regular monitoring and report to Governors
Head Teacher and Senior Leaders	• Ensure that all staff receive suitable CPD to carry out their e-Safety roles • Create a culture where staff and learners feel able to report incidents • Ensure that there is a system in place for monitoring e-Safety • Follow correct procedure in the event of a serious e-Safety allegation being made against a member of staff or pupil • Inform the local authority about any serious e-Safety issues • Ensure that the school infrastructure/network is as safe and secure as possible • Ensure that policies and procedures approved within this policy are implemented • Use an audit to annually review e-Safety with the school's technical support **(Appendix 3)**
e-Safety Leader	• Lead the Health & Safety Working Party • Log, manage and inform others of e-Safety incidents • Lead the establishment and review of e-Safety policies and documents • Ensure all staff are aware of the procedures outlined in policies relating to e-Safety • Provide and/or broker training and advice for staff • Attend updates and liaise with the LA e-Safety staff and technical staff • Meet with Senior Leadership Team and e-Safety Governor to regularly discuss incidents and developments • Coordinate work with the school's designated Child Protection Coordinator
Teaching and Support Staff	• Participate in any training and awareness raising sessions • Read, understand and sign the Staff AUP • Act in accordance with the AUP and e-Safety Policy

	• Report any suspected misuse or problems to the e-Safety Leader • Monitor ICT activity in lessons, extracurricular and extended school activities
Pupils	• Read, understand and sign the Pupil AUP and the agreed class internet rules • Participate in e-Safety activities, follow the AUP and report any suspected misuse • Understand that the e-Safety Policy covers actions out of school that are related to their membership of the school
Parents and Carers	• Endorse (by signature) the Pupil AUP • Discuss e-Safety issues with their child(ren) and monitor their home use of ICT systems (including mobile phones and games devices) and the internet • Access the school website in accordance with the relevant school AUP • Keep up to date with issues through newsletters and other opportunities • Inform the Headteacher of any e-Safety issues that relate to the school
Technical Support Provider	• Ensure the school's ICT infrastructure is as secure as possible • Ensure users may only access the school network through an enforced password protection policy for those who access children's data • Maintain and inform the Senior Leadership Team of issues relating to filtering • Keep up to date with e-Safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse can be reported to the e-Safety Leader for investigation • Ensure monitoring systems are implemented and updated • Ensure all security updates are applied (including anti-virus and Windows)

EDUCATION OF PUPILS

A progressive planned e-Safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited.

- Key e-Safety messages are reinforced through assemblies, Safer Internet Day (February), class visits and assemblies by the Police Community Support Officer (PCSO) and throughout all lessons.
- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies.
- Pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to

reduce the likelihood of coming across unsuitable material. Pupils are aware of the need to report any inappropriate or unsuitable material
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches. Staff pre-check any searches.
- Pupils are taught to be critically aware of the content they access on-line and are guided to validate the accuracy and reliability of information
- Pupils are taught to respect copyright when using material accessed on the internet
- Pupils sign an AUP every other school- year, which will be shared with parents and carers. Parents and Carers will sign an AUP on behalf of EYFS and KS1 Pupils.

EDUCATION AND INFORMATION FOR PARENTS AND CARERS

Parents and carers will be informed about the ways the internet and technology is used in school.
They have a critical role to play in supporting their children with managing e-Safety risks at home, reinforcing key messages about e-Safety and regulating their home experiences. The school supports parents and carers to do this by:

- Providing clear AUP guidance which they are asked to sign with their children and regular newsletter and web site updates
- Raising awareness through activities planned by pupils
- Inviting parents to attend activities such as e-Safety assemblies or other meetings as appropriate.

TRAINING OF STAFF AND GOVERNORS

There is a planned programme of e-Safety training for all staff and governors to ensure they understand their responsibilities as outlined in this policy and the AUPs. This includes:

- An annual audit of the e-Safety training needs of **all** staff
- **All** new staff receiving e-Safety training as part of their induction programme
- This e-Safety Policy and its updates being shared and discussed in staff meetings.
- The e-Safety Leader providing guidance and training as required to individuals and seeking support on issues.
- Staff and governors are made aware of the UK Safer Internet Centre helpline 0844 381 4772

CYBER BULLYING

Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's Anti-Bullying Policy.

- The school will follow procedures in place to support anyone in the school community affected by cyber bullying
- All incidents of cyber bullying reported to the school will be recorded
- The school will follow procedures to investigate incidents or allegations of cyber bullying
- Pupils, staff and parents and carers will be advised to keep a record of the bullying as evidence
- The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.
- Pupils, staff and parents and carers will be required to work with the school to support the approach to cyber bullying and the school's e-Safety ethos
- Sanctions for those involved in cyber bullying will follow those for other bullying incidents and may include:

  - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content
  - Internet access may be suspended at the school for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or AUP.
  - Parent and carers of pupils will be informed
  - The police will be contacted if a criminal offence is suspected

TECHNICAL INFRASTRUCTURE

The person(s) responsible for the school's technical support will ensure that the following guidelines are adhered to:

- The School ICT systems are managed in ways that ensure that the school meets e-Safety technical requirements
- There are regular reviews and audits of the safety and security of school ICT systems
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:
  - the downloading of executable files by users
  - the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of school
  - the installing programs on school devices unless permission is given by the technical support provider or ICT coordinator
  - the use of removable media (e.g. memory sticks) by users on school devices.
  - the installation of up to date virus software

- Access to the school network and internet will be controlled with regard to:
  - users having clearly defined access rights to school ICT systems through group policies
  - users being provided with a username and password
  - users being made aware that they are responsible for the security of their username and password and must not allow other users to access the systems using their log on details
  - users must immediately report any suspicion or evidence that there has been a breach of security
  - an agreed process being in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system. Guests are not routinely allowed access to network, volunteers must sign a volunteer agreement.
  - Key Stage 1 pupil's access to the internet will be by adult demonstration with directly supervised access to specific and approved online materials
  - Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and activities which will be adult directed

- The internet feed will be controlled with regard to
  - the school maintaining a managed filtering service provided by an educational provider (TRUSTnet)
  - the school monitoring internet use
  - requests from staff for sites to be removed from the filtered list being approved by the Senior Leadership Team and logged using the Proforma found in the e-Safety folder on the teacher share area **(Appendix 4)**
  - requests for the allocation of extra rights to users to by-pass the school's proxy servers being recorded, agreed and logged
  - any filtering issues being reported immediately e-Safety Leader or the school technician

- The ICT System of the school will be monitored with regard to:
    - the school ICT technical support regularly monitoring and recording the activity of users on the school ICT systems
    - e-Safety incidents being documented and reported immediately to the e-Safety Leader who will arrange for these to be dealt with immediately in accordance with the AUP

DATA PROTECTION

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. The school will:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- use personal data only on secure password protected computers and other devices
- ensure that users are properly "logged-off" at the end of any session in which they are
- accessing personal data
- store or transfer data using secure data transfer systems, encryption and secure password protected devices
- make sure data is deleted from the device or SLP once it has been transferred or its use is complete

USE OF DIGITAL AND VIDEO IMAGES

Photographs and video taken within school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school's website or learning platform and to provide information about the school on the website. The school will:

- When using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites
- Allow staff to take images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.
- Camera phones should not be used for creating or transferring images of children and young people without the express permission of the School Leadership Team.
- Make sure that images or videos that include pupils will be selected carefully and will not provide material that could be reused
- Make sure that pupils' full names will not be used anywhere on the school website, particularly in association with photographs
- Written permission from parents or carers will be obtained before images or videos of pupils are electronically published
- Not publish pupils' work without their permission and the permission of their parents.
- Keep the written consent where pupils' images are used for publicity purposes, until the image is no longer in use
- Publish a policy regarding the use of photographic images of children which outlines policies and procedures. **(Appendix 5)**

COMMUNICATION (INCLUDING USE OF SOCIAL MEDIA)

A wide range of communications technologies have the potential to enhance learning. The school may (if applicable):

- **with respect to email**
    - Ensure that all school business will use the official school email service
    - Ensure that any digital communication between staff and staff, pupils or parents and carers (email, chat, VLE etc) is professional in tone and content
    - Make users aware that email communications may be monitored
    - Inform users what to do if they receive an email that makes them feel uncomfortable, is

offensive, threatening or bullying in nature
  - Provide whole class or group email addresses for use at Key Stage 1
  - Provide pupils at Key Stage 2 and above with individual school email addresses for educational use only
  - Teach pupils about email safety issues through the scheme of work and implementation of the AUP
  - Ensure that personal information is not sent via email
  - Only publish official staff email addresses

- **with respect to social media**
- Control access to social media and social networking sites
- Provide staff with the tools to risk assess sites before use and check the sites terms and conditions to ensure the site is age appropriate
- Make sure that staff official blogs or wikis will be password protected and run from the school website with approval from the Senior Leadership Team
- Advise / remind parents and carers of national expectations through newsletters, letters, parent consultations and meetings
  Publish information and share learning experiences on a school Facebook/Twitter account, if one is created in the future

- **with respect to personal publishing**
  Teach pupils via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible
- Advise all members of the school community not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory
- Register concerns regarding pupils' use of email, social networking, social media and personal publishing sites (in or out of school) and raise with their parents and carers, particularly when concerning pupils' underage use of sites
- Discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction
- Outline safe and professional behaviour

with respect to mobile phones

- Allow staff to bring mobile phones into school as long as they are turned off or on silent and must only use them during break, lunchtimes or when they are not in contact with pupils' unless they have the permission of the Headteacher.
- Staff are not allowed to use their mobile phone to take photographs or video in school for any purpose without the express permission of the Senior Leadership Team (a list of those permitted in Appendix 7)
- Advise staff not to use their personal mobile phone to contact pupils, parents and carers
- Provide a mobile phone for activities that require them
- Pupils are allowed to bring mobile phones into school but they must be handed into the school office or their teacher at the start of the day. It is the responsibility of the pupil to collect the phone at the end of the day

ASSESSMENT OF RISK

Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances the school will examine and adjust the e-Safety Policy. Part of this consideration will include a risk assessment:

- looking at the educational benefit of the technology
- considering whether the technology has access to inappropriate material

However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from internet use.

All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990
and breaches will be reported to Police.

REPORTING AND RESPONSE TO INCIDENTS

The school will follow the West Sussex County Council's flowchart **(Appendix 6)** to respond to illegal and inappropriate incidents as listed in those publications

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyber bullying, illegal content etc)
- The e-Safety Leader will record all reported incidents and actions taken in the School e-Safety incident log and in any other relevant areas e.g. Bullying or Child Protection log
- The designated Child Protection Coordinator will be informed of any e-Safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures.
- The school will manage e-Safety incidents in accordance with the Positive Behaviour Policy where appropriate
- The school will inform parents and carers of any incidents or concerns in accordance with school procedures
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact West Sussex Safeguarding Team and escalate the concern to the police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding for Schools Adviser, Local Authority Designated Officer (LADO) or West Sussex County Council Senior ICT Adviser

If any incident or concern needs to be passed beyond the school then the concern will be escalated to the Children's Safeguarding Manager.	**Children's Safeguarding Manager** Rosemary Terry 01243 777926
Should serious s-Safety incidents take place, the following external persons and agencies should be informed:	**Local Authority Designated Officer (LADO)** 033022 23339 **Police** **MASH (Multi-Agency Safeguarding Hub) 01403 229900** **West Sussex Children's Access Point (CAP)** 01403 229900 **ICT in Schools Officer**

	Simon Gawn 033022 25926

The police will be informed where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on materials, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images
- Promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist material

SANCTIONS AND DISCIPLINARY PROCEEDINGS

Sanctions and disciplinary procedures will be taken where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography, adult or mature content
- promotion of any kind of discrimination, racial or religious hatred
- personal gambling or betting
- personal use of auction sites
- any site engaging in or encouraging illegal activity
- threatening behaviour, including promotion of physical violence or mental harm
- 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
- using school systems to run a private business
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords)
- creating or propagating computer viruses or other harmful files

In addition the following indicates school policy on these uses of the Internet:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
On-line gaming (educational)		✓		
On-line gaming (non-educational)				✓
On-line gambling				✓
On-line shopping / commerce			✓	
Webchats / Facetime		✓		
Video Conferencing		✓		
File sharing (using p2p networks)				✓

P2P file sharing allows users to access media files such as books, music, movies, and games using a specialized P2P software program that searches for other connected computers on a P2P network and locates the desired content. The nodes (peers) of such networks are end-user computer systems that are interconnected via the Internet.

SANCTIONS FOR MISUSE: PUPILS

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. internal / external exclusion
Deliberately accessing or trying to access material that could be considered illegal	✓	✓	✓		✓	✓		✓
Unauthorised use of non-educational sites during lessons	✓	✓			✓		✓	
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓			✓		✓	
Unauthorised use of social networking / instant messaging / personal email	✓	✓			✓		✓	
Unauthorised downloading or uploading of files	✓	✓			✓		✓	
Allowing others to access school network by sharing username and passwords	✓	✓			✓		✓	
Attempting to access or accessing the school network, using another pupil's account	✓	✓			✓		✓	
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓			✓		✓	
Corrupting or destroying the data of other users	✓	✓			✓		✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓			✓		✓	
Continued infringements of the above, following previous warnings or sanctions	✓	✓			✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓			✓		✓	

Using proxy sites or other means to subvert the school's filtering system	✓	✓		✓	✓	✓		
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓		✓	✓			
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓	✓	✓	✓
Receipt or transmission of materials that infringes the copyright of another person or infringes the Data Protection Act	✓	✓			✓		✓	

SANCTIONS FOR MISUSE: STAFF

Incidents:	**Refer to Headteacher**	**Refer to Local Authority / HR**	**Refer to LADO (L) / Police (P)**	**Refer to technical support staff for action re filtering / security**	**Warning**	**Suspention**	**Disciplinary action**
Deliberately accessing or trying to access material that could be considered illegal	✓	✓	L, P		✓	✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓				✓		
Unauthorised downloading or uploading of files	✓				✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network using another person's account	✓				✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓				✓		
Deliberate actions to breach data protection or network security rules	✓	✓			✓		
Corrupting or destroying the data of others users or causing deliberate damage to hardware or software	✓		P				✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to staff	✓	✓			✓		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to learners	✓	✓	L		✓	✓	✓
Breach of the school e-safety policies in relation to communication with learners	✓		L		✓		

Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils	✓		L		✓		
Use personal camera phone to take photographs / videos of pupils without the express permission of the Senior Leadership Team	✓	✓	L, P		✓	✓	✓
Actions which could compromise the staff member's professional standing	✓				✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓				✓		
Using proxy sites or other means to subvert the school's filtering system	✓				✓		
Accidentally accessing offensive or pornographic material and failing to report the incident	✓		L		✓		
Deliberately accessing or trying to access offensive or pornographic material	✓		L				✓
Breaching copyright or licensing regulations	✓				✓		
Continued infringements of the above, following previous warnings or sanctions	✓		In some cases P				✓

Appendix 1a

Pupil Acceptable Use Policy

All pupils must follow the rules in this policy when using school computers.

Pupils that do not follow these rules may find:

- They are not allowed to use the computers,
- They can only use the computers if they are more closely watched.

Their teachers will show pupils how to use the computers.

	Computer Rules
1	I will only use polite language when using the computers.
2	I must not write anything that might: upset someone or give the school a bad name.
3	I know that my teacher will regularly check what I have done on the school computers.
4	I know that if my teacher thinks I may have been breaking the rules they will check on how I have used the computers before.
5	I must not tell anyone my personal information.
6	I must not tell my username and passwords to anyone else but my parents.
7	I must never use other people's usernames and passwords or computers left logged in by them.
8	If I think someone has learned my password then I will tell my teacher.
9	I must log off after I have finished with my computer.
10	I know that e-mail is not guaranteed to be private. I must not send unnamed e-mails.
11	I must not use the computers in any way that stops other people using them.
12	I will report any websites that make me feel uncomfortable to my teacher or a member of staff.
13	I will tell my teacher or a member of staff straight away if I am sent any messages that make me feel uncomfortable.
14	I will not try to harm any equipment or the work of another person on a computer.
15	If I find something that I think I should not be able to see, I must tell my teacher straight away and not show it to other pupils.

UNACCEPTABLE USE

Examples of unacceptable use include, but are not limited to:

- Using a computer with another person's username and password.
- Creating or sending on the Internet any messages that might upset other people.
- Looking at, or changing work that belongs to other people.
- Waste time or resources on school computers.

✂ -

Pupil User Agreement Form for the Pupil Acceptable Use Policy

I agree to follow the school rules when using the school computers. I will use the network in a sensible way and follow all the rules explained by my teacher.

I agree to report anyone not using the computers sensibly to my teacher.

I also agree to tell my teacher or another member of staff if I see any websites that that make me feel unhappy or uncomfortable.

If I do not follow the rules, I understand that this may mean I might not be able to use the computers.

Pupil Name: ____ Class: ____________

Pupil Signature: ____

(Years 3, 4, 5, and 6 only)

I have read, understood and explained the Acceptable Use Policy to my child and I am happy for my child to use the Internet.

I realise that any pupil under reasonable suspicion of not following these rules when using (or misusing) the computers may have their use stopped, more closely monitored or past use investigated.

Parent/Carers/Guardians Name: _______________________________________

Parent/Carers/Guardians Signature: _______________________________ Date: ___________

Appendix 1b

Name of School	**Lyminster Primary School**
AUP review Date	**February 2019**
Date of next Review	**February 2020**
Who reviewed this AUP?	**Kim Jones (SBM)**

Please adapt as appropriate for the group of staff / systems at your school.

Acceptable Use Agreement: Staff, Volunteers, Governors & Contractors

Covers use of all digital technologies while in school: i.e. email, internet, intranet, network resources, learning platform, software, communication tools, social networking tools, school website, apps and other relevant digital systems provided by the school or school umbrella body (Local Authority, Academy, Free School Trust, etc).

Also covers school equipment when used outside of school, use of online systems provided by the school or school umbrella body when accessed from outside school, and posts on social media made from outside school premises/hours which reference the school or which might bring your professional status into disrepute.

Lyminster Primary School regularly reviews and updates all AUP documents to ensure that they are consistent with the school Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may therefore be subject to monitoring.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password and change my passwords regularly. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.

- I will not allow unauthorised individuals to access email / internet / intranet / network / social networks / mobile apps / or any other system I have access to via the school or school umbrella.
- I will ensure all documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
  This is currently: *LGfL StaffMail / TRUSTnet TrustMail*
- I will only use the approved method/s of communicating with pupils or parents/carers: *email system (*: *LGfL StaffMail, LondonMail/ TrustMail)*, and only communicate with them in a professional manner and on appropriate school business.
- I will not support or promote extremist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the appropriate line manager / school named contact *[Mrs Kim Jones]*.
- I will not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other ICT 'defence' systems*.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.
- I will follow the school's policy on use of mobile phones / devices at school and will ensure that my device is inaccessible to children.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.
- I will only I take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.
- I will use the school's Learning Platform or online cloud storage service in accordance with school protocols.
- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will only access school resources remotely (such as from home) using the *LGfL / school approved system* and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I am aware that under the provisions of the GDPR (General Data Protection Regulation), my school and I have extended responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the school's data policy and adequately protected. The school's data protection officer must be aware of all data storage.

- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the relevant Senior Member of Staff / Designated Safeguarding Lead Mrs Gemma Terrill.
- I understand that all internet and network traffic / usage can be logged and this information can be made available *to the Head* / *Safeguarding Lead* on their request.
- I understand that internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.
- *Staff that have a teaching role only:* I will embed the school's online safety / digital literacy / counter extremism curriculum into my teaching.

Acceptable Use Policy (AUP): Agreement Form

All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / safeguarding policies.

I understand that if the school has loaned me a laptop, the Laptop remains the property of Lyminster Primary School, and I will return it promptly should I no longer be working/volunteering for the school.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature .... Date ....

Full Name .... (printed)

Job title / Role ....

Appendix 1C Volunteer/Helper Acceptable Use Policy

School networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. All users are required to follow the conditions laid down in the policy.

Conditions of Use

Personal Responsibility

Users are responsible for their behaviour and communications. Volunteers/helpers will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will report any misuse of the network a member of staff.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Below is a set of rules that must be complied with. This is not an exhaustive list.

1	I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school (or West Sussex County Council) into disrepute.
2	I will use appropriate language –I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3	I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4	Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person (see 21). I will not reveal any of my personal information to students.
5	I will not trespass into other users' files or folders.
6	I will ensure that I log off after my network session has finished.
7	I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school leadership team.
8	I will not use the network in any way that would disrupt use of the network by others.
9	I will report any accidental access, receipt of inappropriate materials or filtering breaches/ unsuitable websites to a member of staff.
10	I will not use "USB drives", portable hard-drives, or personal laptops on the network without having them "approved" by the school and checked for viruses.
11	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
12	I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.
13	I will support and promote the school's e-safety and Data Security policies and help students be safe and responsible in their use of the Internet and related technologies.

14	I will not send or publish material that violates Data Protection Act or breaching the security this act requires for personal data, including data held on the SIMS Learning Gateway.
15	I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.
16	I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
17	I will ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

Users are expected to inform a member of staff immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on the school's network will be regularly checked by the ICT Technician. Users identified as a security risk will be denied access to the network.

✂ -

Volunteer/Helper User Agreement Form for the Volunteer/Helper Acceptable Use Policy

As a school user of the network resources, I agree to follow the school rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the School Business Manager or ICT Technician.

I agree to report any misuse of the network to the Headteacher or School Business Manager.

I also agree to report any websites that are available on the school Internet that contain inappropriate material to the Headteacher or School Business Manager.

Lastly I agree to ensure that portable equipment such as cameras or laptops will be kept secured when not in use and to report any lapses in physical security to the Headteacher or School Business Manager.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that volunteer/helper under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Volunteer/Helper Name: ____

Volunteer/Helper Signature (if appropriate): ________________________________

Date: _ _ /_ _ /_ _ _ _

Lyminster Primary
Health & Safety Working Party Terms of Reference

PURPOSE

To provide a consultative group that has wide representation from the Lyminster Primary School, with responsibility for monitoring and promoting of Health & Safety (including E-Safety) across the school , including the impact of any initiatives. The group will also be responsible for regular reporting to the Full Governing Body.

MEMBERSHIP

The Health & Safety Working Party will seek to include representation from all stakeholders.
The composition of the group includes:

- Headteacher
- Child Protection/Safeguarding officer
- Business Manager
- e-Safety Leader
- Parent Governor
- ICT Technical Support staff

Other people may be invited to attend the meetings to provide advice and assistance where necessary.
Working Party members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.
Working Party members must be aware that many issues discussed by this group could be of a sensitive or confidential nature. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the room.

DURATION OF MEETINGS

Meetings shall be held termly. A special or extraordinary meeting may be called when and if deemed necessary.

FUNCTIONS

- To keep up to date with new developments in the area of Health & Safety including e-safety via West Sussex Services for Schools site and/or other communication channels
- To annually review and develop the Health & Safety and E-safety policies in line with new technologies and incidents
- To monitor the delivery and impact of the policies
- To monitor log of reported Health & Safety & E-safety incidents (anonymous) to inform future areas of
- teaching/learning/training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of Health & Safety. This could be carried out through:
    - Staff meetings
    - Pupil forums (for advice and feedback)
    - Governors meetings
    - Website/VLE/Newsletters
    - E-safety events
    - Internet Safety Day (annually held on the second Tuesday in February)
- To monitor Internet sites used across the school
- To monitor filtering/change control logs (e.g. requests for unblocking sites)
- To monitor the safe use of data across the school
- To monitor incidents involving cyber-bullying for staff and pupils

AMENDMENTS
The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all Working Party members, by agreement of the majority.

The above Terms of Reference for Lyminster Primary School have been agreed
signed by

Member of SLT: ___________________________________

Date: _______________

Date for review: __________________

Calendar of duties
There will be standing items in each meeting which may include:
Review of Health & Safety and E-safety incidents, preparation of materials for publication (website/newsletter etc)

Autumn
Overview of issues encountered last year and resolutions
Allocation of responsibilities for the year
Discussion on Safer Internet Day ideas and allocation of tasks
Review and Report on staff training needs
Spring
Review and report on incidents (including cyber-bullying)
Report on preparations or review of Safer Internet Day
Distribution of Parent / Carer / Student e-Safety questionnaire
Examination of the latest issues around e-safety
Summer
Report on Student voice and e-safety / questionnaire responses
Review and report of e-safety education throughout the school
Review and report on filtering and Internet issues throughout the year
Review of Health and Safety and E-safety policies
Recommendations for future work

Lyminster Primary School e-Safety Audit

Area of Concern		Y	N	Comment
Passwords and Personal Data	Do all learners, users and members of staff have and use individual usernames and passwords?	**Y**	**N**	**Staff have individual log-ons and passwords which change regularly The children have Generic passwords**
	Is there a guest logon for visitors / supply teachers?	**Y**		
	Are users with generic usernames and passwords (e.g. KS1 / EYFS) always supervised?	**y**		
	Are all computers protected by passwords?	**Y**		
	Are all staff passwords of a complex nature (containing upper and lowercase and numbers)?	**Y**		
	Do staff change their password if they think it is known by another party?	**Y**		
	Are all devices for staff use only protected with passwords / PINs (e.g. iPads)?	**Y**		
	Have all removable devices that store personal data been encrypted (e.g. laptops / USB sticks)?	**Y**		**School provides encrypted memory sticks to staff**
	Are the administrative passwords up to date and available to those with permission to access them, including a member of the school's leadership team?	**Y**		
	Are there any logged incidents due to misuse of passwords?		**N**	

Area of Concern		**Y**	**N**	**Comment**
Filtering and Monitoring	Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe and secure access?	**Y**		**Trustnet**
	Are there any devices that do not use the school's filtering system?		**N**	
	Is there a list of the sites the school have allowed / denied? Does a member of the SLT approve requests to unblock a site?	**Y**		
	Can the filtering be differentiated for pupils / staff?	**Y**		
	Is there a list of the most popular sited visited?	**Y**		
	Is it possible to monitor the filtering logs? Is this done regularly and by whom?	**Y**		
	Is there a list of the filtered sites that users have attempted to access but access has been denied?	**Y**		
	Is there a list of those people who have permission to bypass the filter?	**Y**		
	Are there any logged filtering incidents?		**N**	
Software Updates	Have all the computers had the latest Operating System (OS) updates installed?	**Y**		
	Are there computers with older OS which are no longer being supported?		**N**	
	Is there a list of software installed on computers?	**Y**		**In the process of updating**

Area of Concern		**Y**	**N**	**Comment**
	Has all the software been updated to the latest versions available?	**Y**		
Hardware Updates	Are all new devices security marked and entered on the equipment inventory?	**Y**		
	Are all new devices loaded with the correct anti-virus software?	**Y**		
	Are the servers functioning effectively?	**Y**		
	Is there any equipment requiring replacement?		**N**	
	Is there a pattern in the logged hardware incidents?		**N**	
Network Security	Is the wireless network secure? Is a wireless key needed to access it?	**Y**		
	Are personal devices allowed on the wireless network?	**Y**		
	Are staff prevented from loading programmes onto their laptop?	**Y**		
	Can removable media be used on workstations? (e.g. USB sticks)	**Y**		
	Is the anti-virus software up to date on all computers?	**Y**		
	Is it possible to monitor what users have completed on the network? Is it possible to identify an individual responsible for misuse?	**Y**		**We now have AB tutor – being installed on all machines which**

Area of Concern		Y	N	Comment
				offers greater monitoring capabiliy
	Are there any logged incidents due to network security or virus issues?		**N**	
Connectivity	Have there been any WAN (Wide Area Network – Internet feed from supplier) issues?		**N**	
	Have there been any LAN (Local Area Network – schools internal network) issues?		**N**	
	Have there been any wireless connectivity issues?		**N**	
	Is there a pattern to logged network connectivity incidents?		**N**	
Technical Staff **(including those teachers with IT responsibilities)**	Are there clear procedures for the monitoring of staff that carry out technical support?		**N**	
	Are there clear procedures in place to support staff when carrying out their role in situations that might involve access to illegal / unsuitable and reporting of incidents?		**N**	
	What help, support or training do the technical team need?			**None**
Developments	What school IT issues / developments have been addressed?			
	What IT developments need to be investigated?			

Area of Concern		Y	N	Comment
	Are the developments being made for educational and e-safety reasons? Can independent support and information be found to validate these developments?			

Signed: ______________________________ **Signed:** ______________________________ **Signed:** ______________________________

Headteacher /SLT **Technician** **IT Governor**

Date:

Welcome to Lyminster Primary School

Appendix 4

Request for Unblocking a Website

Website: www.___________________________________ Member of staff requesting change: __________________________ Date: __________

Purpose of site: ____ To be used by year group: ____________

Area		Y/N	Why should this website be unblocked?
Curriculum	Is there a clear curriculum reason to allow this site?		
Nature of Materials	Are the materials on the website suitable for this age range (and not contentious in nature)?		
Endorsement	Should the school endorse this site?		
Social	Does the site have social aspects that allow communication between users?		
Outside of School	Should users have unsupervised and / or unfiltered access to this site outside of school hours?		
Reliability	Has the website been created by a reliable source?		
Age Restrictions	Does the website have any age restrictions?		
Materials	Does the school retain the rights to materials uploaded onto the site?		
Privacy	Is access to materials limited to selected groups?		
Registration	Do users have to register to use the site?		

SLT Decision:

Approved / Declined Signed:________________________________ Initials: ________ Date: ______________

Appendix 5

Key Policy Points:

- Lyminster Primary School recognises that a balance between the low risk of misuse and the numerous positive results of colourful, well produced school material is necessary.
- The school will only take and use images (photographs, videos and DVDs) that are appropriate and are considered to be safe from misuse.
- Children will be made aware of why their pictures are being taken and how they will be used.
- The school will take extra precautions to ensure that only appropriate images are used for the website and Twitter feed.
- If it is found that a camera phone has been misused, the school will follow its usual disciplinary procedures.
- If an image of a child is used, the child's name **will not** be published. If a name is published, **no image will be used** without specific consent.
- Parents and legal guardians will be asked to sign an agreement that any images they take during school activities will not be used inappropriately

If you wish to see the full policy document please ask for a copy at the school office or access this on the school website under 'about us > policies'

PARENTS

Please read our Policy for the Use of Images of Children and indicate whether you agree to your child's images being taken. You have the option to indicate whether or not you consent to your child's images being taken and used for different purposes. **You can withdraw your consent at any time by writing to the school.**

Name of child (block capitals)		Year group	
Child's date of birth			
Name of parent or legal guardian (block capitals)			
I have read the school's policy on the use of images of children and I agree to its provisions. *Please give your consent by putting your initials next to each statement. Your child's images will not be taken/used specified, if you do not give your consent.*			
I give my consent to images of my child being taken and used for official school purposes of promoting or publicising school events in accordance with the guidelines of the policy for the duration of their time at the school.			*Please initial here*
I give my consent to images of my child being used on the school website and Twitter feed and I understand that these images will be available on the World Wide Web.			
I give my consent for images taken by the school in accordance with the guidelines of the policy to be used for official West Sussex County Council publications.			
I give my consent to my child being included in any images taken by other parents or carers who wish to photograph or record school events in which their children are participating. *All parents or legal guardians will be asked to sign an agreement for appropriate use of images they take during school events. Please see below.*			
I agree that any photographic or video images I as a parent or legal guardian might take at school events will not be used inappropriately.			
Signature of parent or legal guardian of the child			
Relationship to the child			
Date (date/month/year)			

NB: There may be other circumstances, falling outside the normal day to day activities of the school, when images of children are needed. The school recognises that in such circumstances specific consent from the parent or legal guardian will be sought before any photography or filming of children starts. If you have concerns or queries about any of this information, please contact the school.

Please return to the School Office as soon as possible

Appendix 6

List of those staff with permission to use their mobile phones to take photographs.

Staff Name	**Role**	**Precise nature of pictures or circumstances for which permission is granted**
Suzanne Prince	IT Technician	To photograph equipment or serial numbers only – no photos including any children or children’s work

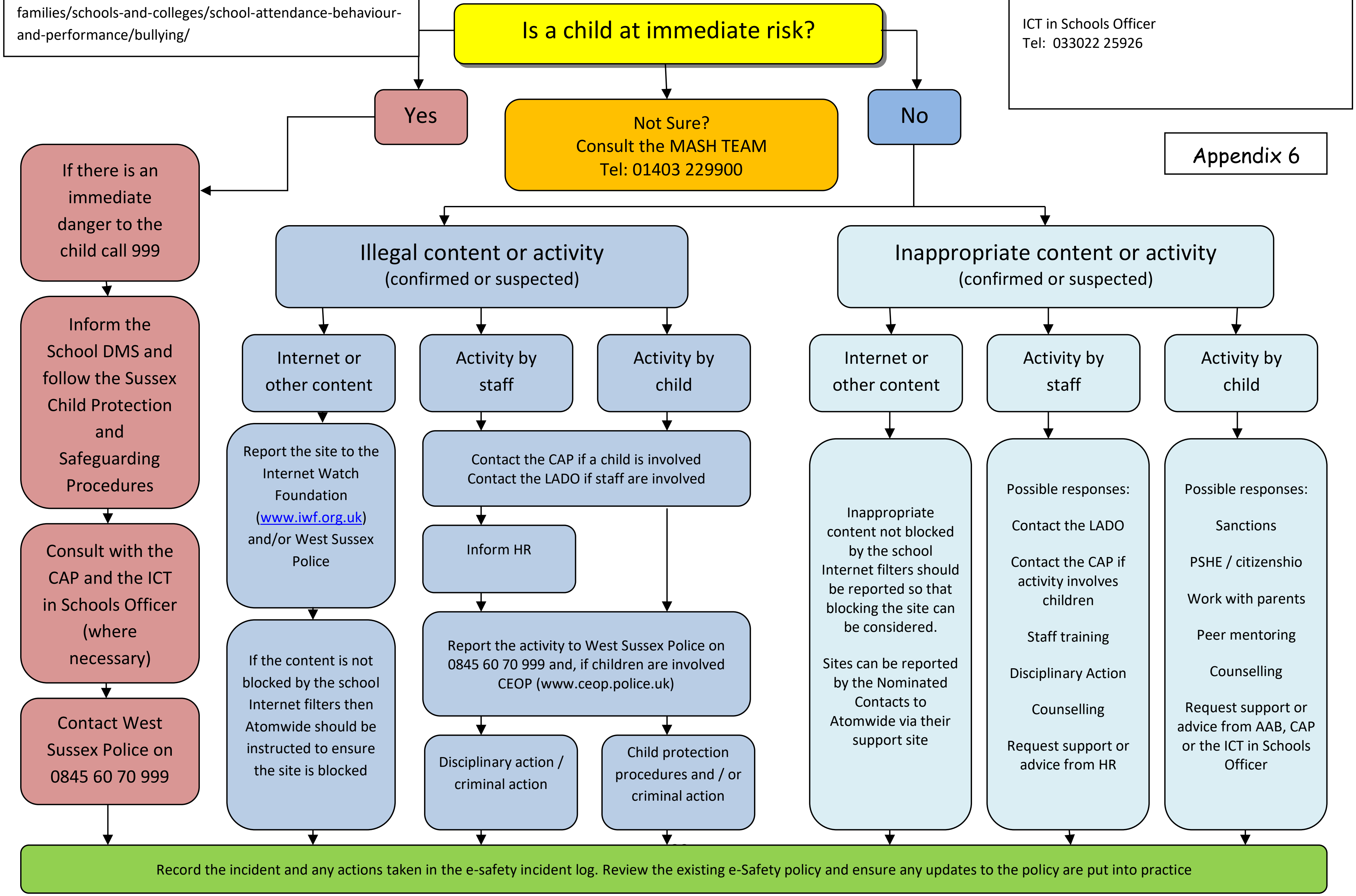
If a School Related e-Safety Incident Occurs

West Sussex MASH) Tel: 01403 229900
West Sussex Action Against Bullying
https://www.westsussex.gov.uk/education-children-and-families/schools-and-colleges/school-attendance-behaviour-and-performance/bullying/

Local Authority Designated Office (LADO) Tel: 033022 23339

ICT in Schools Officer
Tel: 033022 25926

Appendix 6



Is a child at immediate risk?

Yes

Not Sure?
Consult the MASH TEAM
Tel: 01403 229900

No

If there is an immediate danger to the child call 999

Inform the School DMS and follow the Sussex Child Protection and Safeguarding Procedures

Consult with the CAP and the ICT in Schools Officer (where necessary)

Contact West Sussex Police on 0845 60 70 999

Illegal content or activity
(confirmed or suspected)

Internet or other content

Activity by staff

Activity by child

Report the site to the Internet Watch Foundation (www.iwf.org.uk) and/or West Sussex Police

If the content is not blocked by the school Internet filters then Atomwide should be instructed to ensure the site is blocked

Contact the CAP if a child is involved
Contact the LADO if staff are involved

Inform HR

Report the activity to West Sussex Police on 0845 60 70 999 and, if children are involved CEOP (www.ceop.police.uk)

Disciplinary action / criminal action

Child protection procedures and / or criminal action

Inappropriate content or activity
(confirmed or suspected)

Internet or other content

Activity by staff

Activity by child

Inappropriate content not blocked by the school Internet filters should be reported so that blocking the site can be considered.

Sites can be reported by the Nominated Contacts to Atomwide via their support site

Possible responses:

Contact the LADO

Contact the CAP if activity involves children

Staff training

Disciplinary Action

Counselling

Request support or advice from HR

Possible responses:

Sanctions

PSHE / citizenshio

Work with parents

Peer mentoring

Counselling

Request support or advice from AAB, CAP or the ICT in Schools Officer

Record the incident and any actions taken in the e-safety incident log. Review the existing e-Safety policy and ensure any updates to the policy are put into practice