St Andrew's CE Primary School
Online Safety Policy
2017

Safeguarding in Education Team
Bolton Safeguarding Children

MISSION STATEMENT

We believe that St. Andrew's C.E. Primary School exists to provide life's main opportunities for our children guided by and learning from the example and teaching of Jesus Christ.
These opportunities come from an ethos and curriculum that provide maximum learning experiences for each individual child, no matter what their particular learning abilities may be.
We will aspire to a curriculum which results in the enjoyment of learning, children who feel good about themselves and in which everyone can be good at something. We will encourage pupils to show tolerance and respect for each other, set themselves high standards, to take pride in their work and do their best.
We will provide curriculum enrichment activities including first hand experiences, creative opportunities, visits and visitors.
We will offer every child the chance to achieve as much as they are able.
We will achieve high standards for all children, giving them secure foundations for future learning and success in life.

Schedule for Development / Monitoring / Review

This Online policy was approved by the *Governors:*	*Autumn 2017*
The implementation of this Online policy will be monitored by the:	*Children's Welfare Governing Body Sub Committee*
Monitoring will take place at regular intervals:	*at least once a year*
The *Governors Sub Committee* will receive a report on the implementation of the Online policy generated by the monitoring group (which will include anonymous details of Online incidents) at regular intervals:	*Insert time period (suggested to be at least once a year*
The Online Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online or incidents that have taken place. The next anticipated review date will be:	*Autumn 2018*
Should serious Online incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager, LA Safeguarding Officer, Police See also ' **Support for Bolton Schools** ' at the end of this policy*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of*
    - *Pupils*
    - *parents / carers*
    - *staff*

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of Pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents

of cyber-bullying, or other online incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the Online Policy and for reviewing the effectiveness of the policy. This will be carried out by the Children's Welfare Sub Committee receiving regular information about online incidents and monitoring reports. A member of the *Governors* has taken on the role of *Online Governor* a part of their role as Safeguarding Governor. The role of the Online Governor will include:

- *regular meetings with the Online Co-ordinator*
- *regular monitoring of online incident logs*
- *reporting to relevant Governors meetings*

Head teacher and Senior Leaders:

- The Head teacher has a duty of care for ensuring the safety (including Online) of members of the school community, though the day to day responsibility for Online will be delegated to the Online Co-ordinator.
- The Head teacher and members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff. (See flow chart on dealing with Online incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR disciplinary procedures).
- The Head teacher is responsible for ensuring that the Online Coordinator and other relevant staff receive suitable training to enable them to carry out their Online roles and to train other colleagues, as relevant.
- The Head teacher 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 monitoring role through allocated 'Tech Time'. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Co-ordinator.

Online Safety leader (Safeguarding lead) :

- takes day to day responsibility for Online issues and has a significant role in establishing and reviewing the school online policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online incident taking place.
- provides support and advice for staff

- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of online incidents and creates a log of incidents to inform future Online developments
- meets regularly with Online Governor to discuss current issues and review incident logs
- attends relevant meeting / committee of Governors if required
- reports regularly to Senior Leadership Team

Any incidents will be reported to the Head teacher who will lead investigations and impose the appropriate sanctions.

Network Manager / Technical staff:

Bolton ICT service will be responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online technical requirements that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online technical information in order to effectively carry out their Online role and to inform and update others as relevant
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher and Computing subject leader for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online matters and of the current school Online policy and practice
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Head teacher and/or Online Coordinator for investigation / action / sanction
- all digital communications with Pupils / parents / carers should be on a professional level and only carried out using official school systems
- Online issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Lead Designated Safeguarding Person (DSP)

The DSP should be trained in Online issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable User Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online practice when using digital technologies out of school and realise that the school's Online Policy covers their actions out of school, if related to their membership of the school

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns through produced literature and parent workshops.

Parents and carers will be encouraged to support the school in promoting good online practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems / website as part of the wider school provision will be expected to bring their own hardware before being provided with access to school systems.

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online provision. Children and young people need the help and support of the school to recognise and avoid online risks and build 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 should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key Online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil Acceptable Use Policy (AUPs) and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that Pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

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

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

- *Curriculum activities*
- *Letters, newsletters, web site,*
- *Parents / Carers evenings / workshops*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications*

Education & Training – 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 and informal online safety training will be made available

to staff. This will be regularly updated and reinforced. An audit of the online training needs of all staff will be carried out regularly. It is expected that some staff will identify Online Safety as a training need within the performance management process.

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- Safeguarding and Computing lead (or other nominated person) will receive regular updates through attendance at external training events (e.g. from / 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 meetings and INSET days.
- Safeguarding and Computing lead (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

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

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

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their Online responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users) will be provided with a username and secure password by *the Computing Subject lead who will keep an up to date record of users and their usernames.*
- The "master / administrator" passwords for the ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place
- The Computing Subject Lead 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
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list.
- The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / management / administration.)

- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

Staff must take full responsibility if their family members are allowed on school devices that may be used out of school.
Staff must not download executable files and installing programmes on school devices.
Removable media (e.g. memory sticks) should not be used by users on school devices.
Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

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

Bring Your Own Device (BYOD)

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

Use of digital and video images

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

- When using digital images, staff should inform and educate Pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other Pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that Pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include Pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

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

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. School Personal Data will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

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

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

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

- The official *school* email service may be regarded as safe and secure. Users should be aware that email communications are monitored. *Staff and Pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).*
- Users must immediately report, to the 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 Pupils or parents / carers (email, text etc.) must be professional in tone and content. *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*

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

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. While, Ofsted's Online framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

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

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

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions, Risk assessment, including legal risk School staff should ensure that:
- No reference should be made in social media to Pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the designated Online safety staff and the external provider (Blippit) to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	

Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)				X	
On-line gaming (non educational)				X	
On-line gambling				X	
On-line shopping / commerce				X	
File sharing			X		
Use of social media				X	
Use of messaging apps				X	
Use of video broadcasting e.g. YouTube				X	

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

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

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

In the event of suspicion, all steps in this procedure should be followed:
Have more than one senior member of staff / volunteer been involved in this process? This is vital to protect individuals if accusations are subsequently reported.

Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

Record any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour the sending of obscene materials to a child adult material which potentially breaches the Obscene Publications Act criminally racist material other criminal conduct,
- activity or materials. Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

School Actions & Sanctions

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

Pupils

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

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

Staff

Incidents:	Refer to Head teacher	Refer to Local Authority Designated Officer	Refer to Police	Refer to Technical Support Staff for	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X			X	X
Inappropriate personal use of the internet / social media / personal email	X			X	X		
Unauthorised downloading or uploading of files	X			X	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			X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X			X	X		
Deliberate actions to breach data protection or network security rules	X	X		X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X		X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X		X	X		X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with Pupils	X	X		X	X		

Actions which could compromise the staff member's professional standing	X				X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X			X	X		X
Using proxy sites or other means to subvert the school's filtering system	X	X		X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X		X	X
Breaching copyright or licensing regulations	X	X			X		
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X

Appendix

EYFS and KS1 Acceptable Use Policy

 My Learning	• I will use school devices (PCs, laptops, tablets/ ipads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.
 My Online Safety	• I will always use what I have learned about Online Safety to keep myself safe. • I will tell a teacher if I see something that upsets me on the screen.
 Using the Internet @school	• I will only use the internet when the teacher says I can. • I will only go on websites that my teacher allows me to. • I will tell my teacher if I go on a website by mistake.
 Using the Internet @home	• I will not share personal information about myself when on-line (names, addresses, telephone numbers, age, gender, school details) • Where I have my own username and password, I will keep it safe and secret. • I will tell a trusted adult if I see something that upsets me on the screen. **My use of Social Media and Gaming** • I understand that certain sites and games have age restrictions to keep me safe. • I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying.

I understand that these rules help me to stay safe and I agree to follow them.
I also understand that if I break the rules I might not be allowed to use the school's computing equipment.
I understand that these rules, help me to stay safe and I agree to follow them.
I also understand that if I break the rules I might not be allowed to use school computing equipment.

_____ _____

Child's Signature **Date**

EYFS, Key Stage 1 Parents / Carers:

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

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

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

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

_____ _____

Parent/Carer's Signature **Date**

Key Stage 2 Pupils Acceptable Use Policy

 My Learning	• I will use school devices (PCs, laptops, tablets/ ipads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly. • When logging on using my own username and password, I will keep it safe and secret. • I will save only school work on the school computer and will check with my teacher before printing. • I will log off or shut down a computer when I have finished using it.
 Using the Internet @school	• I will only visit sites that are appropriate to my learning at the time **My School Accounts** • I will keep my username and password safe and secure - I will not share it. • I will not 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. **My role as a Digital Citizen.** • I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to a trusted adult. • I will respect other people's work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission. • I will not take or distribute images of anyone without their permission.
 Using the Internet @home	• I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, school details) • If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me. • I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line, to a trusted adult or online agencies e.g.: CEOP, Childnet, Childline, Barnardos. **My Communications (Including texting and messaging)** • I will be aware of "stranger danger", when I am communicating online. • I will be polite and responsible when I communicate with others. • I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions. **My use of Social Media and Gaming** • I understand that certain sites and games have age restrictions to keep me safe. • I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying.

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

I understand that these rules, help me to stay safe and I agree to follow them.

I also understand that if I break the rules I might not be allowed to use school computing equipment.

My parents/carers understand that keeping me safe on the internet at home is their responsibility.

_____

Child's Signature

KS2 Parents / Carers:

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

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

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

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

_____ _____

Parent/Carer's Signature **Date**

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 lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used (please tick as appropriate):-

☐	School Display
☐	Records of Achievement
☐	School Publicity e.g. local or national press or media
☐	Use on the school website
☐	Use on the school Facebook account

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other Pupils in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree

Digital / Video Images Permission Form

Parent / Carers Name

Student / Pupil Name

Signed

Date

Staff (and Volunteer) Acceptable Use Policy Agreement

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

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 ICT 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 ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for Pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that Pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online in my work with young people.

For my professional and personal safety:

- I understand that the *school* will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, texts etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school ICT 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 ICT systems
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with Pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and restricted data must be held in lockable storage.
- I understand that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law 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:

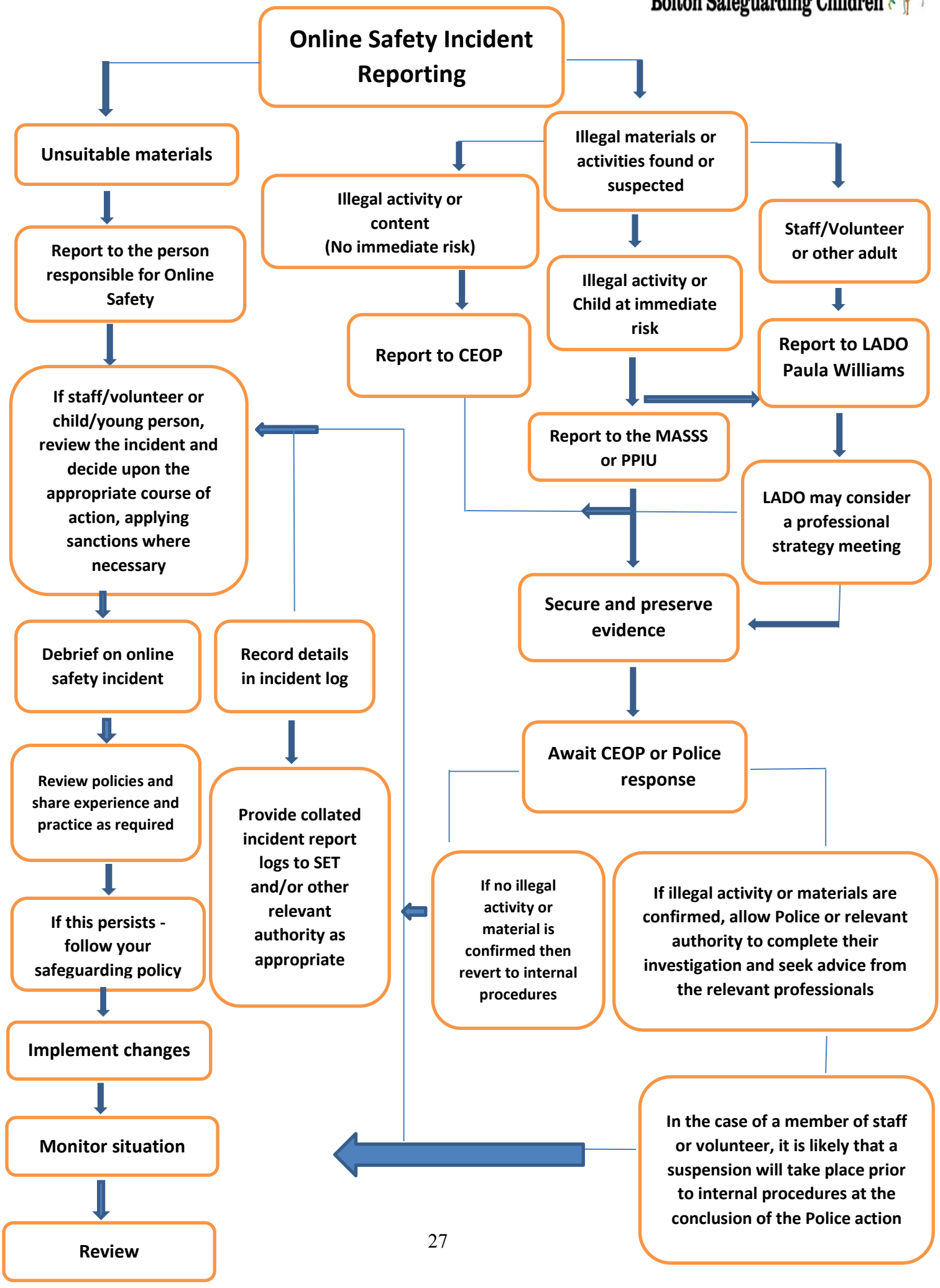
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include (schools / academies should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to Governors / Directors 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 ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date


Online Safety Incident Reporting
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
If this persists - follow your safeguarding policy
Implement changes
Monitor situation
Review
Record details in incident log
Provide collated incident report logs to SET and/or other relevant authority as appropriate
Illegal activity or content (No immediate risk)
Report to CEOP
Illegal materials or activities found or suspected
Illegal activity or Child at immediate risk
Report to the MASSS or PPIU
Staff/Volunteer or other adult
Report to LADO Paula Williams
LADO may consider a professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professionals
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the Police action

Support Contacts for Bolton Schools

SET – Safeguarding in Education Team:

- Jacqui Parkinson – Safeguarding in Education Officer – 01204 337472
- Natalie France – Safeguarding Education Social Worker – 01204 331314

LADO: Paula Williams - 01204 337474

Bolton's MASSS – 01204 331500

Police protection investigation unit – 0161 856 7949

Community Police - 101

EXIT Team – 01204 337195

Bolton Safeguarding Children's Board: Shona Green – 01204 337964

If there is an ICT network issues contact your school ICT provider.

If your provider is Bolton School ICT Unit – contact 01204 332034 or contact@sict.bolton.gov.uk

Support for Bolton Schools

SET – Safeguarding in Education Team:

- Jacqui Parkinson – Safeguarding in Education Officer – 01204 337472
- Natalie France – Safeguarding Education Social Worker – 01204 331314

LADO: Paula Williams - 01204 337474
Bolton's MASSS – 01204 331500
Police protection investigation unit – 0161 856 7949
Community Police - 101
EXIT Team – 01204 337195
Bolton Safeguarding Children's Board: Shona Green – 01204 337964

If there is an ICT network issues contact your school ICT provider.
If your provider is Bolton School ICT Unit – contact 01024 332034 or contact@sict.bolton.gov.uk

Bolton Information Management Unit - Tasadiq.Naveed@bolton.gov.uk

http://mossextranet.bolton.gov.uk/website/pages/DataProtectionandFreedomofInformation.aspx

ONLINE INCIDENT LOG

Details of ALL Online incidents to be recorded by the Online Lead within your School, this incident log will be monitored weekly by a senior member of staff.

Date & time	Name of child or staff member	M / F	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons