Little Lever School

ASPIRE ACHIEVE EXCEL

Online Safety Policy

Development of this Policy

The Online policy has been developed by the Bolton Safeguarding in Education team and the online safety group with advice from the South West Grid for Learning Trust (SWGfL). The school has adopted and adapted the model policy in consultation with SLT, Governors and the safeguarding committee.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of students when they are off the *trust's* school sites 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 trust's schools, but is linked to membership of the trust. 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 *trust* 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

The following section outlines the online safety roles and responsibilities of individuals and groups within the *trust*:

Board of Trustees:

Trustees are responsible for the approval of the Online Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Trustees* receiving regular information about online incidents and monitoring reports. A member of the *Board* has taken on the role of *Online Governor* or part of the overall Safeguarding Governor role. The role will include:

- *regular meetings with the safeguarding lead*
- *regular monitoring of online incident logs*
- *regular monitoring of filtering / change control logs*
- *reporting to relevant Trustees meeting*

Principal and Senior Leaders:

The *Principal* 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 *Operations director*.

- The Head teacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff. (See flow chart on dealing with Online incidents – included in appendix).

- *The Head teacher / Senior Leaders are responsible for ensuring that the Operations director 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 / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*

- *The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the Operations director.*

Online Safety subject leader (Designated Safeguarding Lead):

- leads on online safety for students
- takes day to day responsibility for Online issues and has a leading 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 training 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 Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
- reports to relevant meetings of *Governors*
- reports regularly to Senior Leadership Team

ICT Manager and Technical staff:

The *ICT Manager and Technical Staff* are responsible for ensuring:

- that the schools' technical infrastructure is secure and is not open to misuse or malicious attack
- that the trust meets required online technical requirements and any Local Authority / other relevant body Online Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering 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 / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher / Safeguardiing lead / Operations director for investigation and possible action and potential sanction
- that monitoring software / systems are implemented and updated in line with the developer.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online matters and of the current *Trust* Online policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the *Designated Safeguarding Lead* for investigation, possible action and potential sanction
- all digital communications with students / 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
- students understand and follow the Online and acceptable use policies
- students 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 students 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*

Child Protection / Designated Safeguarding Lead

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

Safeguarding Committee

The committee provides a consultative group with responsibility for issues regarding Online and the monitoring the online policy including the impact of initiatives. The committee will also be responsible for regular reporting to the *trustees*.

Members of the *committee* will assist the Operations director *(or other relevant person)* with:

- the production, review and monitoring of the school online policy and documents.
- *the production, review and monitoring of the school filtering policy and requests for filtering changes.*
- mapping and reviewing the online curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students about the online provision
- monitoring improvement actions identified through use of safeguarding audits

Students / pupils:

- are responsible for using the *trust* digital technology systems in accordance with the 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 and 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 *trust* will take every opportunity to help parents understand these issues through *parents' evenings, letters, website / VLE and information about national and local online safety initiatives.* Parents and carers will be encouraged to support the *Trust* 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 / VLE and on-line student records
- their children's personal devices in the trust (where this is allowed)

Policy Statements

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students* to take a responsible approach. The education of *students* 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 pastoral activities
- Students should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- *Students should be helped to understand the need for the student 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 students 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 students 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, web site, VLE*
- *Parents / Carers evenings and school events*
- *High profile events and campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites and publications e.g.*

www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

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.
- 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.
- *Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events (e.g. from LA or other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This Online safety policy and its updates will be presented to and explained to staff.*
- *Designated Safeguarding Lead (or other nominated person) will provide advice, guidance and training to individuals as required.*

Training – Governors / Directors

Governors should take part in online training and awareness sessions, with particular importance for those who are members of any subcommittee or group involved in technology, Online safety, health and safety and 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 and information sessions for staff or parents.

.

Technical – infrastructure / equipment, filtering and monitoring

The school works closely with the Local Authority in establishing appropriate filtering mechanisms. It is the responsibility of the school to ensure that all the online measures ae carried out, as suggested below. The school should also check their Local Authority policies on these technical issues, and the technical policies of other relevant agencies.

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 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 of the Local Authority and other relevant bodies.
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- 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 *ICT staff who will keep an up to date record of users and their usernames.* Users are responsible for the security of their username and password *and will be required to change their password regularly.*
- The "administrator" passwords for the trust ICT system, used by the ICT Manager (or other person) must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place (e.g. school safe)
- The ICT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- 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. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- *The school has provided enhanced and differentiated user-level filtering.*

- *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.*
- *Users are encouraged to report any actual or potential technical incident or security breach to the ICT manager or Operations director.*
- 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 appropriate account is available for the provision of temporary access of "guests", trainee teachers, supply teachers, visitors) onto the school systems.

A policy is in place regarding the extent of personal use that users (staff / students / community users) and their family members are allowed on school devices that may be used out of school.

A policy is in place that allows staff to downloading executable files and installing programmes on school devices.

A policy is in place regarding the use of removable media (e.g. memory sticks, CDs, DVDs) 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.

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. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students 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 students 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 *students* 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 students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- *Students must not take, use, share, publish or distribute images of others without their permission*
- *Photographs published on the website, or elsewhere that include students will be selected carefully.*
- *Written permission from parents or carers will be obtained before photographs of* students are published on the school website / social media
- *Student's work can only be published with the permission of the student 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.

The school must ensure that:

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

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.

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

- the device must be password protected if possible
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete
- The official *school* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. *Staff and students should therefore use only the trust email service to communicate with others when in school, or on school systems (e.g. by remote access).*
- Users must immediately report, to the ICT Manager the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to and such communication.
- Any digital communication between staff and students or parents / carers (email, chat, VLE etc.) must be professional in tone and content. *These communications may only take place on official (monitored) trust systems. Personal email addresses, personal text messaging or personal social media must not be used for these communications.*
- *Students 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 trust website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

There is an increase in use of all types of social media for professional and personal purposes. Staff should be mindful and manage risk and behaviour online. It is important for staff to follow the key principles for 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. Staff should be referring to these documents.

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.

The *school's* use of social media for professional purposes will be checked regularly by the safeguarding committee to ensure compliance with 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 the 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	X		
Use of messaging apps		X	X		
Use of video broadcasting e.g. YouTube		X	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 (below and appendix) for responding to online safety incidents and report immediately to the Designated Safeguarding Lead or 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 trust 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 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 records (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 and other criminal conduct, activity or materials.

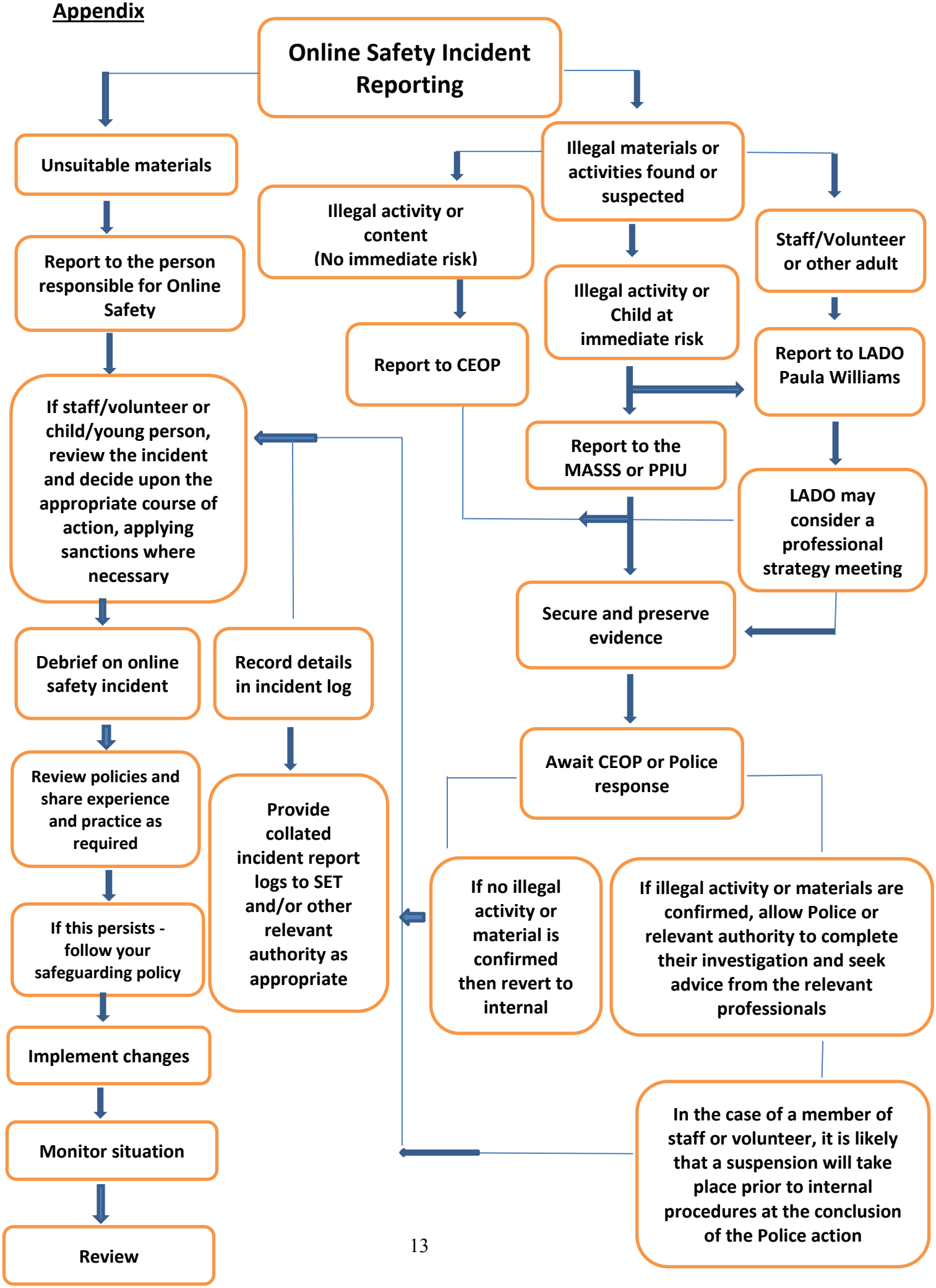
In these instances the computer in question should be isolated as best you can. Any change to its state may hinder a later police investigation.

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

School Actions and 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.

Appendix


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
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

Policy Statements

Search:

Students are allowed to bring mobile phones or other personal electronic devices to school but must not be visible or used during the school day.

Senior staff, year leaders and form tutors have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.
Searching with consent - such staff may search with the student's consent for any item.
Searching without consent - such staff may only search without the student's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or is contrary to the rules of the school.

Staff should not normally carry out any search of a student, a student's possessions or electronic device without first seeking guidance from the Designated Safeguarding lead or a member of the Senior Leadership Team. Staff may carry out a search without doing this if they believe serious harm will be caused to a person if a search is not carried out immediately.

In carrying out the search:
The member of staff must have reasonable grounds for suspecting that a *student* is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.

The member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search.

The member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the student being searched.

The member of staff carrying out the search must be the same gender as the *student* being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the *student* being searched.

There is a limited exception to this rule: staff can carry out a search of a *student* of the opposite gender including without a witness present, **but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.**

Extent of the search:
The person conducting the search may not require the *student* to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).
'Possessions' means any goods over which the *student* has or appears to have control – this includes desks, lockers and bags.

A student's possessions can only be searched in the presence of the *student* and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices
A member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so.

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. It is important that staff should have training and sufficient knowledge of electronic devices and data storage.

If inappropriate material is found on the device it is up to the member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- **Child sexual abuse images (including images of one child held by another child)**
- **Adult material which potentially breaches the Obscene Publications Act**
- **Criminally racist material**
- **Material relating to other criminal conduct, activity or materials**

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more senior leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.

The school should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff.

Deletion of Data
Following an examination of an electronic device, if the member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

A record should be kept of the reasons for the deletion of data.

Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices (particularly given the possible high value of some of these devices).

Confiscated items should be stored securely in the main school office.