STAFF, VISITOR AND VOLUNTEER ACCEPTABLE USE POLICY 2025

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

THE 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 and personal use.
- That school IT 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 IT in their everyday work.

The school will ensure that staff and volunteers will have good access to IT to enhance their work, to enhance learning opportunities for children's learning and will, in return, expect staff and volunteers to agree to be responsible users.

ACCEPTABLE USE AGREEMENT

I understand that I must use the school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of the use of technology for enhancing learning and will ensure that children receive opportunities to gain from the use of IT. I will, educate the young people in my care in the safe use of technology and be a good role model in my own use of all digital technologies in my work with young people.

FOR MY PROFESSIONAL AND PERSONAL SAFETY:

- I understand that the school will monitor my use of the IT systems, email and other digital communications;
- I understand that the rules set out in this agreement also apply to use of school IT systems (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- School data will **not** be stored on external hard drives or USB storage devices
- I will not support or promote extremist organisations, messages, or individuals;
- I will not give a voice or opportunity to extremist visitors with extremist views;
- I will not browse, download, or send material that is considered offensive or of an extremist nature by the school;
- I understand that the school IT systems are primarily intended for educational use only
- 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 DSL.
- I will be professional in my communications and actions when using school IT systems.
- I will not access, copy, remove or otherwise alter any other user's files, without their expressed 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 /social media platforms) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with children/parents/carers using official school systems. I will not use my personal work email to communicate with parents. This is to protect my workload. 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 LOCAL AUTHORITY HAVE THE RESPONSIBILITY TO PROVIDE SAFE AND SECURE ACCESS TO TECHNOLOGIES:

- When I use personal 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's equipment. I will also follow any additional rules set by the school about such use, including not using personal devices in front of children. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will request access to the guest Wi-Fi if completing work for school use only. I will disconnect from the school WI-FI immediately after the work has been completed. The password for the guest WI-FI will be updated at least half termly.
- I will not use personal email addresses on the school IT 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 by fully closing down the computer each day
- 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 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.
- I will only transport, hold, disclose, or share personal information about myself or others, as outlined in the School Personal Data Policy. **Where digital personal data is transferred outside the secure local network, it must be encrypted.** Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

WHEN USING THE INTERNET IN MY PROFESSIONAL CAPACITY OR FOR SCHOOL SANCTIONED PERSONAL USE:

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

I UNDERSTAND THAT I AM RESPONSIBLE FOR MY ACTIONS IN AND OUT OF THE SCHOOL:

I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT 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/academy.

I understand that if I fail to comply with this Acceptable Use Policy, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the Police.

STAFF PASSWORDS:

- All staff users will be provided with a username and password by Bolton Schools ICT who will keep an up to date record of users and their usernames.
- A password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters and must not include proper names or any other personal information about the user that might be known by others

SOCIAL MEDIA POLICY – See social media policy for more details. Summary below:

- It is not appropriate for representatives of the school to have children for which they have a duty of care who are under the age of 18 as 'friends' on such sites.
- Staff, governors and volunteers who have accounts on social networking sites must ensure the highest level of security is in place and that they do not either accept or make a friend request to any person under the age of 18 years to whom they have acted 'in a position of trust' (including ex-pupils)
- Those who work with children and young people are at an increased risk of allegations being made against them. It is therefore vital that staff and volunteers take appropriate steps to protect themselves from allegations, and to ensure appropriate behaviour both online and offline.
- There is an uneven power base between staff, governors and volunteers and young people, in which adults have authority over students (current and former) which continues to shape those relationships.
- The relationship with pupils should at all times remain professional, and staff, governors and volunteers must not correspond with pupils through such sites or add them as 'friends'.
- All staff, governors and volunteers are responsible for their own actions and behaviour and must avoid any contact which would lead any reasonable person to question their motivation and intent.
- Under no circumstances must staff, governors and volunteers accept friend requests from children, young people or pupils, nor should they make such requests.

- Should a young person attempt to contact you in this way, you should make this known to the Head Teacher immediately.
- Think very carefully about what you share with friends, even if your information is 'private' as this may appear on your 'friends' page
- Protect your mobile phone with a PIN in case it gets lost or stolen, and so that your social networking account is further protected

DO NOT:

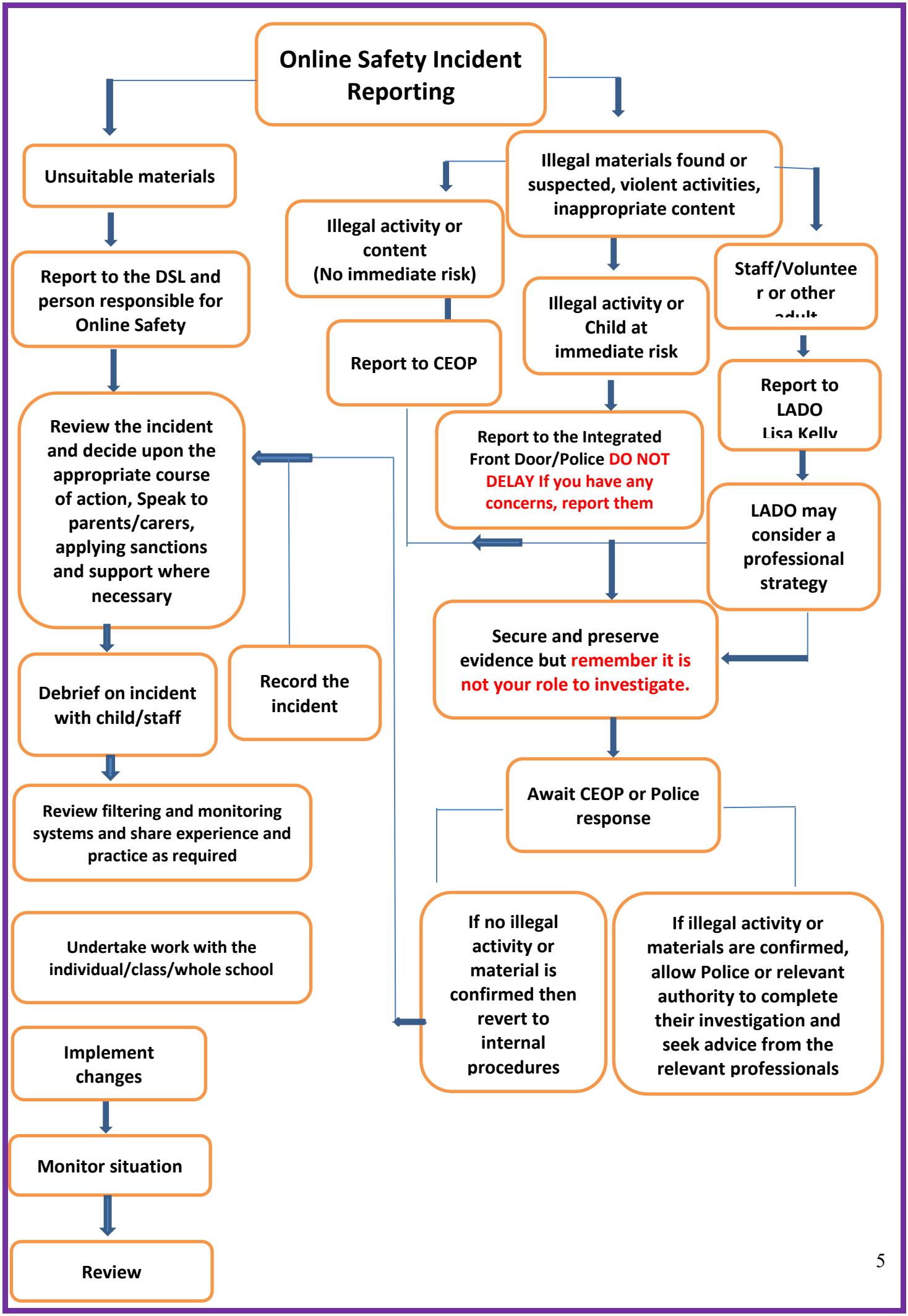
- Share information that shows you or your friends in a compromising situation
- Post images of pupils or parents on personal social media
- Post content that may be seen as racist, homophobic, bullying or threatening
- Bring the school into disrepute by posting derogatory, threatening or inappropriate comments about the school, the school community or your colleagues
- Access social networking sites from school computers
- Access social networking sites from personal devices during working hours

REPORTING ONLINE SAFTEY INCIDENTS

See below a flow chart on what to do if an online safety incident needs reporting.

A record must be added on CPOMs (for children) and reported to the DSL. The same record of information must be given to DSL regarding staff members.

- Date and Time
- Name of child/staff member
- Room and computer device/number
- Details of incident including evidence
- Actions and reasons


Online Safety Incident Reporting
Unsuitable materials
Report to the DSL and person responsible for Online Safety
Review the incident and decide upon the appropriate course of action, Speak to parents/carers, applying sanctions and support where necessary
Debrief on incident with child/staff
Record the incident
Review filtering and monitoring systems and share experience and practice as required
Undertake work with the individual/class/whole school
Implement changes
Monitor situation
Review
Illegal materials found or suspected, violent activities, inappropriate content
Illegal activity or content (No immediate risk)
Report to CEOP
Illegal activity or Child at immediate risk
Report to the Integrated Front Door/Police DO NOT DELAY If you have any concerns, report them
Staff/Volunteer or other adult
Report to LADO Lisa Kelly
LADO may consider a professional strategy
Secure and preserve evidence but remember it is not your role to investigate.
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

I have read and understand the above and agree to use the school IT systems (both in and out of school) and my own devices (in school and when conducting communications related to the school) within these guidelines. Please complete smart log to confirm this.