# ONLINE SAFETY POLICY

| | |
|---|---|
| Academic Year | • 2020-21 |
| Staff Consultation | • November 2020 |
| Approved by the Governing Body | • November 2020 |
| The online safety 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 safety or incidents that have taken place. The next anticipated review date will be: | • September 2021 |
| Designated Safeguarding Lead (DSL)<br>Deputy DSLs | • Tracy Lawson<br>• Sara Cardno, Rebecca Johnson, Lyndsey Zammit, Nigel Cross, Gail McGreehin, Ray Baker |
| Online Safety Curriculum Lead | • Rebecca Johnson |
| Online Safety Project Lead | • Rachael Hoyle |
| Safeguarding Governor | • Lynne Davies |
| The Governing Body will receive a report on the implementation of the Online Safety Policy (which will include anonymous details of online safety incidents) at regular intervals: | • Annually |
| Should serious online safety incidents take place the following external persons and agencies should be informed as appropriate: | • The Police, Children's Social Care, Local Authority Designated Officer (LADO) |

## Introduction

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited/filtering)
- Surveys/questionnaires/feedback of
    - students
    - parents/carers
    - staff

## Scope of the Policy

This policy applies to all members of the Lytham St Annes (LSA) High School community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of school/academy digital technology systems, both in and out of School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students 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 online-bullying or other online safety incident covered by this policy which may take place outside of, but is linked to, 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 be taken over issues covered by the School Behaviour Policy. LSA High School will deal with such incidents within this policy and associated Behaviour and Respect & Anti-Bullying Policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

**Contents**

| **Roles & Responsibilities** | |
|---|---|
| **Governing Body** | The Governing Body is responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of the Safeguarding Governor (which includes Online Safety). The role of the Safeguarding Governor will include:<br>• attendance at safeguarding meetings (where online safety will be discussed)<br>• monitoring of online safety incident logs<br>• auditing and monitoring of filtering logs<br>• reporting to the Governing Body |
| **Headteacher & Senior Leadership Team** | The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Designated Safeguarding Lead.<br><br>The Headteacher 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 safety allegation being made against a member of staff.<br><br>The Headteacher is responsible for ensuring that the Designated Safeguarding Lead(s) and other relevant staff (including Year Leaders) receive suitable training and support to enable them to carry out their online safety roles and to train other colleagues as required. |
| **Designated Safeguarding Lead** | • takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents<br>• ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.<br>• provides training and advice for staff<br>• liaises with the Local Authority and other external agencies as required<br>• liaises with school technical staff, the Online Safety Project Lead and the Online Safety Curriculum Lead.<br>• Monitors online safety incidents logged on the School's online referral system (CPOMS) and uses this information to inform future online safety developments (in liaison with the Deputy Head (Pastoral), Safeguarding Team, Online Safety Curriculum Lead and Online Safety Project Lead). Online safety incidents are dealt with and investigated by class teachers or Year Leaders (as appropriate) and investigations/actions/sanctions will be undertaken by them with the support of the Designated Safeguarding Lead(s) where required.<br>• Audits the monitoring of the internet filtering system (monitored by Year Leaders)<br>• reports regularly to the Headteacher and Governing Body. |

| | |
|---|---|
| | Designated Safeguarding Lead/Deputies:<br>Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:<br>• sharing of personal data<br>• access to illegal/inappropriate materials<br>• inappropriate on-line contact with adults/strangers<br>• potential or actual incidents of grooming<br>• online-bullying<br><br>Respond to referrals made via the online referral system (CPOMS) or in communication with students, parent/carers, staff and professionals from other agencies.<br><br>Support Year Leaders where required in their investigation, action of online safety concerns and manage online safety incidents where there are serious child protection/safeguarding issue<br><br>Audit regularly the monitoring of the internet filtering system to ensure incidents requiring further investigation have been followed up, logged and actioned by the Year Leaders. |
| **Assistant Business Manager responsible for IT/Facilities** | Those with technical responsibilities are responsible for ensuring:<br>• that the school's technical infrastructure is secure and is not open to misuse or malicious attack<br>• that the school meets required online safety technical requirements and any statutory and Local Authority online safety policy/guidance that may apply.<br>• that users may only access the networks and devices through a properly enforced password protection policy<br>• the filtering system is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person<br>• that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant<br>• that the use of the network/internet is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Designated Safeguarding Lead for investigation/action/sanction and that the monitoring/software systems are implemented and updated as agreed (providing the filtering system report daily to Year Leaders and other identified key members of School staff)<br>• . |
| **Teaching and Support Staff** | are responsible for ensuring that:<br>• they have an up to date awareness of online safety matters and of LSA's Online Safety Policy and practices (and other related school policies).<br>• they have read, understood and signed the staff acceptable use agreement.<br>• they report any suspected misuse or problem to the Designated Safeguarding Lead(s) and Year Leader via CPOMS (Safeguarding & Child Protection Policy refers) for |

| | |
|---|---|
| | investigation/action/sanction. The incident should be logged as a CP referral or information and ALSO as an online safety incident.<br>• all digital communications with students and parents/carers should be on a professional level and only carried out using official school systems and within a school working day.<br>• online safety issues are embedded in all aspects of the curriculum and other activities<br>• students understand and follow the Online Safety Policy and acceptable use policies<br>• students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations<br>• 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<br>• in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and ensure that processes are in place for dealing with any unsuitable material that is found in internet searches |
| **Online Safety Curriculum Lead** | is responsible for<br>• mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression and compliance with statutory requirements where appropriate with regard to any identified needs (from recent online safety referrals, current issues etc). |
| **Online Safety Project Lead** | is responsible for:<br>supporting the Designated Safeguarding Lead and Online Safety Curriculum Lead by:<br>• sourcing relevant, purposeful and engaging content to assist with online safety lesson plans,<br>• seeking guidance and information for students, parents/carers and school staff to support online safety and address any prevalent online safety concerns and<br>• communicating with students/ parents/carers and school staff via various methods (school website, twitter, emails, texts, newsletters, assemblies/form time presentations) to provide information, advice and guidance on keeping safe and behaving respectfully and appropriately online. |
| **Year Leaders** | are responsible for:<br>• responding to online safety concerns reported to them via the online referral system (CPOMS) or in communication with students, parent/carers, staff and professionals from other agencies. Where required this may be alongside a Designated Safeguarding Lead/Deputy.<br>• will carry out investigations/actions and may provide sanctions (this may be alongside a Designated Safeguarding Lead/Deputy or member of the Senior Leadership Team).<br>• monitoring the internet filtering system report when received and following up on any concerns that may arise from this report: logging the incident, actions and outcomes on CPOMS as an online safety incident. |

| | |
|---|---|
| **Students** | • are responsible for using LSA High School's digital technology systems in accordance with the student acceptable use agreement<br>• have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations<br>• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so<br>• are 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 online-bullying.<br>• should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the School's Online Safety Policy covers their actions out of school if related to their membership of the school. |
| **Parents/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. LSA High School will take every opportunity to help parents understand these issues through information provided on the school website, via newsletters, social media, letters, parents' evenings and information about national/local online safety campaigns/literature.<br>Parents and carers are encouraged to support LSA High School in promoting good online safety practice and to follow guidelines on the appropriate use of:<br>• digital and video images taken at school events<br>• access to parents' sections of the website/learning platforms and on-line student records<br>• Their online activity with other members of the school community. |
| **The Online Safety Group** | is a consultative group that has wide representation from the School community with responsibility for issues regarding online safety and the monitoring of the Online Safety Policy including the impact of initiatives. This Group, in turn, will feedback to the School's Safeguarding Team. Members will include the Online Safety Curriculum Lead, Designated Safeguarding Lead/Deputy, a Year Leader, Assistant Business Manager for IT & Facilities, Online Safety Project Lead and representation from the staff, parent and student body. The group will also be responsible for regular reporting to the Governing Body.<br>Members of the Online Safety Group will assist with:<br>• the production/review/monitoring of the school online safety policy/documents.<br>• consulting stakeholders – including parents/carers and the students about the online safety provision<br>• monitoring improvement actions |

| **Policy Statements** | |
|---|---|
| **Education - Students** | The education of students in online safety/digital literacy is an essential part of the school's online safety provision. LSA High School will support students by helping them to recognise and avoid online safety risks and build their resilience.<br>The online safety curriculum will be provided in the following ways:<br>• A planned online safety curriculum will be provided as part of PSHE/Computing/other lessons and key messages will be regularly revisited<br>• Key online safety messages will be delivered and reinforced as part of a planned programme of assemblies and tutor time activities<br>• Students will 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.<br>• Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet<br>• Students will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.<br>• Students will be encouraged to adopt safe and responsible online activity both within and outside school.<br>• in lessons where internet use is pre-planned staff will guide students to sites checked as suitable for their use and ensure they have processes in place for dealing with any unsuitable material that is found in internet searches.<br>• Where students are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the students visit.<br>• It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Team 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** | School will seek to provide information and awareness to parents/carers in the following ways to inform parent/carers about:<br>• online safety risks and issues,<br>• how to help keep their children) safe online and<br>• how to respond if their child(ren) comes across potentially harmful and inappropriate material and situations online.<br>• Letters, newsletters, web site, Learning Platform<br>• Parents/carers evenings/sessions<br>• High profile events/campaigns e.g. Safer Internet Day<br>• Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers<br><br>Information provided via the school website and social media platforms will also be available to the wider school community. |

| | |
|---|---|
| **Education & Training – Staff & Volunteers** | It is essential that all staff understand their responsibilities as outlined in this policy. Training will be offered as follows:<br>• A planned programme of safeguarding training that includes online safety training will be made available to staff. This will be regularly updated and reinforced and bespoke/individual training will be provided where the need arises.<br>• Online safety training (the Online Safety Policy, Staff Code of Conduct, Respect & Anti Bullying Policy, Safeguarding & Child Protection Policy amongst others) will be provided to new staff as part of the induction process ensuring that they fully understand LSA High School's policies and procedures, their role and responsibilities and acceptable use agreements.<br>• Relevant School staff (the Headteacher and Senior Leadership Team, the Designated Safeguarding Lead, Online Safety Curriculum Lead, Online Safety Project Lead) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.<br>• This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions. |
| **Training - Governors** | Governors will take part in online safety training/awareness sessions with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:<br>• Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation (e.g. SWGfL).<br>• Participation in school training/information sessions. |
| **Technical – infrastructure/equipment, filtering and monitoring** | LSA High School will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that processes and procedures approved within this policy are implemented and will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:<br>.<br>• School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.<br>• There will be regular reviews and audits of the safety and security of school technical systems<br>• Servers, wireless systems and cabling will be securely located and physical access restricted<br>• All users will have clearly defined access rights to school technical systems and devices.<br>• All users will be provided with a username and secure password by the IT Team. Users are responsible for the security of their username and password.<br>• Assistant Business Manager responsible for IT/Facilities is responsible for ensuring that software licence logs are accurate and up to date and that the number of licences purchased match 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. |

| | |
|---|---|
| | • Internet filtering/monitoring will ensure that children are safe from terrorist and extremist material when accessing the internet.<br>• School 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<br>• Users should report any actual/potential technical incident/security breach to the Assistant Business Manager for IT/Facilities.<br>• 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 devices are protected by up to date virus software.<br>• An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers (similar to permanent members of staff), supply teachers (similar to permanent staff where this is longer term and they are given access), visitors (guest network)) onto the school systems.<br>• Protocols are 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.<br>• Protocols are in place that prevents staff from downloading executable files and installing programmes on school devices without clearance from the Assistant Business Manager for IT/Facilities.<br>• Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Removal devices for storing information should not be used for this purpose. |
| **Mobile Technologies** | Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network.<br>The School Mobile Phone (Devices) Policy refers and links to other School policies which should be considered when using mobile devices. These include but are not limited to the Safeguarding and Child Protection Policy, Behaviour Policy, Respect & Anti-Bullying Policy, Staff Code of Conduct and acceptable user agreements (and any addendums that may exist):<br>• The school acceptable user agreements for staff, students and parents/carers gives consideration to the use of mobile technologies. |
| **Use of Digital and Video Images** | 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 online-bullying 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.<br>• When using digital images, staff will 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.<br>• Written permission from parents/carers will be obtained before photographs of students are published on the school website/social media/local press. |

| | |
|---|---|
| | • 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 is 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.<br>• 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.<br>• 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.<br>• Students must not take, use, share, publish or distribute images of others without their permission<br>• Students' full names will not be used anywhere on a website or blog particularly in association with photographs.<br>• Student's work can only be published with the permission of the student and parents/carers. |
| **Data Protection** | Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.<br><br>LSA High School;<br>• has a Data Protection Policy<br>• implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.<br>• has paid the appropriate fee Information Commissioner's Office (ICO) and the School's Data Protection Officer is named in the Data Protection Policy.<br>• has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.<br>• has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it<br>• the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded<br>• holds only 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. The school implements a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. |

| | |
|---|---|
| | • Ensures personal data held is accurate and up to date where this is necessary for the purpose it is processed for.<br>• Has systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals<br>• Provides staff, parents, volunteers and students with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)<br>• Has procedures in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to have a copy of the personal data held about them (subject to certain exceptions which may apply).<br>• Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)<br>• IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners<br>• has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.<br>• understands how to share data lawfully and safely with other relevant data controllers.<br>• reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.<br>• Has a Freedom of Information Policy which sets out how it will deal with FOI requests.<br>• all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.<br>When personal data is stored on any mobile device or removable media the:<br>• data must be encrypted and password protected.<br>• device must be password protected. (be sure to select devices that can be protected in this way) |

| | |
|---|---|
| | • device must be protected by up to date virus and malware checking software<br>• data must be securely deleted from the device, in line with school/academy policy (below) once it has been transferred or its use is complete.<br>Staff must ensure that they:<br>• at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse<br>• can recognise a possible breach, understand the need for urgency and know who to report it to within the school<br>• can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school<br>• where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.<br>• will not transfer any school/academy personal data to personal devices except as in line with school policy<br>• access personal data sources and records 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. |
| **Communications** | A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks and disadvantages and when they may be used.<br><br>When using communication technologies LSA High School considers the following as good practice:<br>• The official School email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.<br>• Users must immediately report to the Designated Safeguarding Lead/Deputies 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.<br>• Any digital communication between staff and students or parents/ carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content and should take place on official (monitored) school systems. Personal email addresses/text messaging from personal phones/social media must not be used. |

| | Staff & Other Adults | | | | Students | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed | Restrictions |
| **Communication Technologies** | | | | | | | | | |
| Mobile phones may be brought to school | x | | | | x | | | | Students may bring phones/mobile devices to school but these must be switched off and in their school bags between 8.15 – 3.15. They are not be used during the school day at any time unless under staff supervision |
| Use of mobile phones in lessons | | x | | | | | x | | Staff - for professional purposes only but to use school devices where possible. Students - Only to be used in lessons for educational purposes with permission from a member of staff |
| Use of mobile phones in social time | x | | | | | | | x | Staff – yes Students – no |
| Taking photos on mobile phones, cameras, devices | | | | x | | | x | | Staff – no (school devices must be used Students - with permission from a member of staff for educational purposes only |
| Use of other mobile devices e.g. tablets, gaming devices | x | | | | | | x | | Staff - for professional purposes only. Students - with permission from a member of staff for educational purposes only |
| Use of personal email addresses in school, or on school network | | x | | | | | | x | Staff - during social time for personal communications only and in-line with school policy. Students – no |
| Use of school email for personal emails | | | | X | | | | x | Staff and students – no |
| Use of messaging apps | | x | | | | | | x | Staff - during social time for personal communications only and in-line with school policy. Students – no |
| Use of social media | | x | | | | | | x | Staff - during social time for personal communications only and in-line with school policy. Students – no |
| Use of blogs | x | | | | | | x | | Staff - for professional purposes only Students - for educational purposes only |

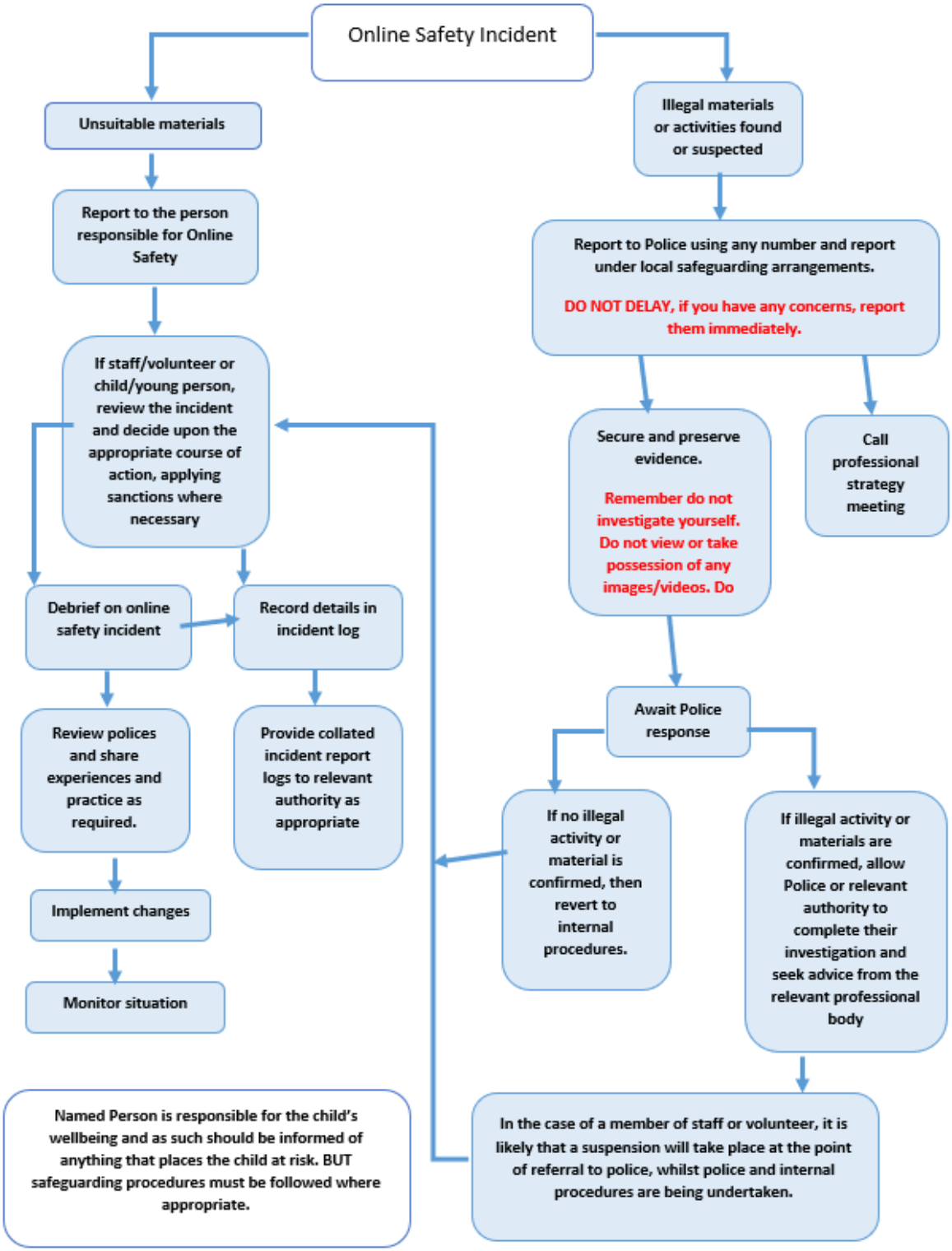
| | |
|---|---|
| **Social Media – Protecting Professional Identity** | With an increase in use of all types of social media for professional and personal purposes this policy sets out clear guidance for staff to manage risk and behaviour online.<br>Core messages include the protection of students, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'.<br>The School and Local Authority have a duty of care to provide a safe learning environment for students and staff.<br>The School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:<br>• Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.<br>• Clear reporting guidance, including responsibilities, procedures and sanctions<br>• Risk assessment, including legal risk<br><br>School staff should ensure that:<br>• No reference should be made in their social media to students, parents and carers or school staff<br>• They do not engage in online discussion on personal matters relating to members of the school community<br>• Personal opinions should not be attributed to the School or Local Authority<br>• Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.<br><br>The school's use of social media for professional purposes is monitored to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies in this document. |
| **Unsuitable and inappropriate activities** | The school believes that the activities referred to in the following table 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: (see page 15/16) |
| **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" on page 15/16).<br><br>See flow chart at page 17 (illegal incidents). |

| 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<br>See also information relating to self-generated images – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges | | | | | X |
| | Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003. | | | | | X |
| | Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 | | | | | X |
| | Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986 | | | | | X |
| | Pornography | | | | X | |
| | Promotion of any kind of discrimination | | | | X | |
| | threatening behaviour, including promotion of physical violence or mental harm | | | | X | |
| | Promotion of extremism or terrorism | | | | X | |
| | Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute | | | | X | |
| Activities that might be classed as cyber-crime under the Computer Misuse Act:<br>• Gaining unauthorised access to school networks, data and files, through the use of computers/devices<br>• Creating or propagating computer viruses or other harmful files<br>• Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)<br>• Disable/Impair/Disrupt network functionality through the use of computers/devices<br>• Using penetration testing equipment (without relevant permission) | | | | | | X |

| | | | | | |
|---|---|---|---|---|---|
| N.B. These type of activities may be reported to the Police. Serious or repeat offences will be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways – further information here | | | | | |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy | | | | X | |
| Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords) | | | | X | |
| Unfair usage (downloading/uploading large files that hinders others in their use of the internet) | | | | X | |
| Using school systems to run a private business | | | | X | |
| Infringing copyright | | | | 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 (staff only) | | X | | | |
| Use of messaging apps (staff only) | | X | | | |
| Use of video broadcasting e.g. Youtube | | X | | | |

**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) 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 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 the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see 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
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - 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 safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

**School actions & sanctions**

It is more likely that 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.