SAINT NICHOLAS SCHOOL

ONLINE SAFETY POLICY

Note: This policy applies to all sections of the school including EYFS

This policy is made available to parents via the school website or on request.

Reviewed December 2020

Review Date December 2021

1. INTRODUCTION

Saint Nicholas School takes online safety very seriously, in the same way as it regards all health & safety issues, safeguarding matters and protection from harm for its pupils.

The law empowers Heads, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is particularly pertinent to online behaviour and Saint Nicholas School will treat seriously all aspects of online safety for its pupils even if they occur out of school hours or offsite.

2. ROLES AND RESPONSIBILITES

Headmaster and Senior Leaders

The Headmaster has a duty of care for ensuring the safety of the school community, and delegates the day to day responsibility for online safety to the E-Learning Coordinator. The Headmaster ensures that the E-Learning Coordinator and other staff receive suitable training to enable them to carry out their online safety roles.

The Headmaster and the Designated Safeguarding Lead (DSL) are aware of procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

E-Learning Coordinator

- takes coordinating responsibility for online safety
- reviews online safety policies / documents
- liaises with Network Manager on implementation of policy
- undertakes relevant CPD and provides training, updates (not less than annually) and advice for staff
- ensures that all staff are aware of the procedures to be followed in the event of an online safety incident
- receives weekly reports from the Network Manager in order to monitor online issues, any online safety incidents, and keep a log to inform future online safety developments
- meets SLT and DSL to discuss current issues, review incident logs as part of the SLT standing agenda

Designated Safeguarding Lead

The DSL is trained in Online Safety issues and is aware of the potential for serious 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

- **Network Manager** ensures that the School's technical infrastructure is secure, meets online safety technical requirements, and is not open to misuse or malicious attack,
- ensures networks and devices are protected by, inter alia, properly enforced password protection,
- keeps up to date with online safety technical information and informs and updates others as relevant,
- ensures internet access is filtered for all users and that illegal content is filtered by employing the internet watch foundation (CAIC) list,
- the School has enhanced differentiated user-level filtering allowing different filtering levels for different groups of users and the network manager monitors use of and activity on online systems and reports findings weekly to the e-learning coordinator.

All Staff

Children and young people need the help and support of the School to recognise and avoid online safety risks and build their resilience.

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum, as follows:

- A planned online safety curriculum (covering, inter alia, staying safe, cyberbullying, radicalisation risks and prevention, and identity protection) is included within Computing / PSHE / Pathways Programme and other lessons,
- Key online safety messages are reinforced in assemblies and tutorial / pastoral activities,
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information, acknowledge the source of information used and to respect copyright,
- Pupils are supported in building resilience to radicalisation as Saint Nicholas School is a safe environment for debating controversial issues and pupils learn how they can influence and participate in decision-making,
- Where pupils are allowed to search the internet freely, staff are vigilant in monitoring the content of the websites visited,
- 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 those sites are temporarily remove from the filtered list for the period of study. Any such instance will be recorded by the Network Manager.

All staff therefore:

- recognise their responsibility for keeping children safe online as elsewhere and follow established protocols for recording and reporting any concern,
- recognise their responsibility to monitor pupils' use of online technology, guide and train them in the safe use of technology and online behaviour, and how to protect themselves in an online context,
- recognise that good practice in all online communication helps improve safety and so all digital communications with pupils and parents must be on a professional level and only carried out using official school systems,
- also recognise that their online behaviour both in and out of school reflects on their professional status and on the reputation of the School. Staff appreciate that care must be taken to avoid inappropriate online activity that would bring them or the school into disrepute. See sections 5 and 6 of this policy for examples and elaboration.

Additionally, it is recognised that all staff need to be vigilant about all aspects of pupils' use of technologies. The opportunities for cyberbullying and the ways in which online bullying can be part of wider bullying behaviour are well known and Saint Nicholas School considers online safety to be part of both its safeguarding and anti-bullying responsibilities. There is a proactive approach to checking hardware and software, and careful monitoring of online activity, but the ongoing awareness of adults who are observant about pupil behaviour and take an interest in what

pupils are doing at all times is as important a safeguard in online activity as it is in all other respects.

Pupils

The pupils at Saint Nicholas School are noted for their responsibility, not only in taking care of themselves but in the concern they have for others. In an online setting they:

- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so,
- know and understand policies on the use of mobile devices, on the taking / use of images and on cyber-bullying,
- understand the importance of adopting good online safety practice out of school and realise that the Online Safety Policy covers their actions out of school, if related to their membership of the School,
- develop effective research skills and appreciate the need to avoid plagiarism, which undermines academic integrity and jeopardises examination results, and to uphold copyright regulations in accordance with the law.

Parents / Carers

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 helps parents understand online safety and good practice through parents' evenings, newsletters, letters, and its website. Parents and carers are encouraged to support the School in promoting good online safety practice and to follow guidelines on:

- digital and video images taken at school events,
- access to parents' sections of the website / Learning Platform and on-line records,
- their children's use of personal devices, both in and out of school.

3. USE OF MOBILE TECHNOLOGIES

All users of a smart phone/personal wifi enabled device in the Saint Nicholas School context should understand that the primary purpose is educational.

The Saint Nicholas School mobile technologies approach is consistent with our other relevant school policies.

Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme as part of PSHEE.

4. USE OF DIGITAL AND VIDEO IMAGES

Staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. There is clear potential for harm or embarrassment to individuals in the short and longer term: these images may provide avenues for cyberbullying; digital images may remain available on the internet forever; employers carry out internet searches for information about potential and existing employees.

Consequently, Saint Nicholas 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 inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images, in particular to recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Guidance from the Information Commissioner's Office is that parents / carers are welcome to take videos and digital images of their own children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should

only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- A pupil's work will only be published with the permission of the pupil and parents.

5. COMMUNICATIONS

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

- The official school email service may be regarded as safe and secure and can be monitored by Saint Nicholas School Network Manager. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school matters,
- Users should be aware that email communications are monitored,
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. Personal email addresses, text messaging or unofficial social media must not be used for these communications,
- Users must immediately report, to the Headmaster, 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,
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff,
- Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use,
- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details, and of the need to communicate appropriately when using digital technologies. They are taught strategies to deal with inappropriate communications.

6. SOCIAL MEDIA - PROTECTING PROFESSIONAL IDENTITY

Saint Nicholas School recognises it has a duty of care to provide a safe learning environment for pupils and staff.

To ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the School, training includes acceptable use, social media risks, checking of settings, data protection, reporting issues. The School also takes steps to ensure that personal information is not published.

Staff members who harass, cyberbully, discriminate on the grounds of any protected characteristics, or who defame a third party may render the *School as well as themselves* liable to the injured party. School staff should ensure that:

- no reference is made in personal social media accounts to pupils, parents / carers or school staff,
- they do not engage in online discussion on personal matters relating to members of the school community,
- personal opinions should not be attributed to the School,
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Personal Use:

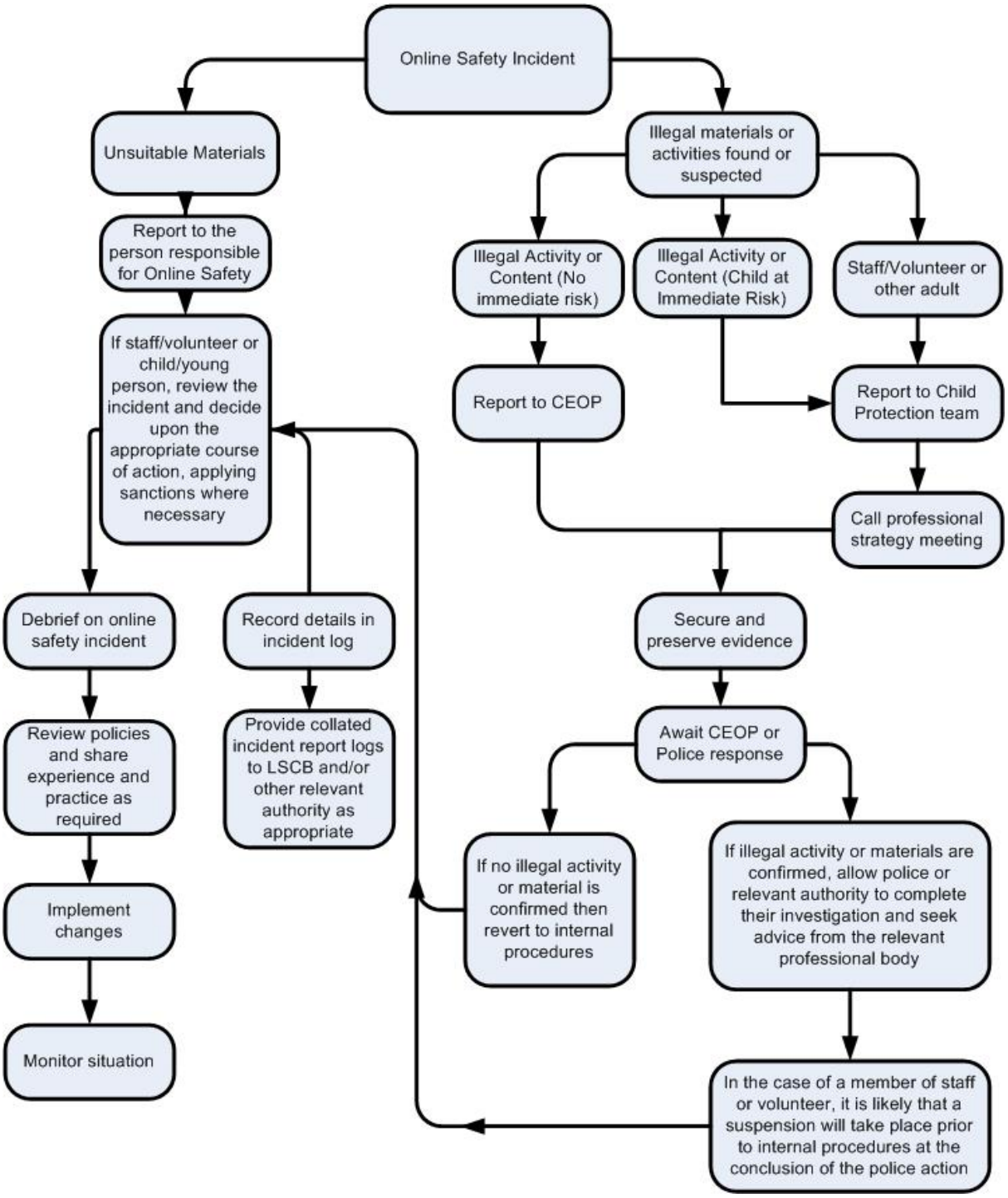
- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the School, it must be made

clear that the member of staff is not communicating on behalf of the School with an appropriate disclaimer. Such personal communications are within the scope of this policy.

- The School permits reasonable and appropriate access to private social media sites, but where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

7. ILLEGAL INCIDENTS

If there is any suspicion that web site(s) 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.



8. OTHER INCIDENTS

It is hoped that all members of the Saint Nicholas 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:

- More than one senior member of staff will be involved in the process. This is vital to protect individuals if accusations are subsequently reported.
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation, then conduct the procedure using a single designated computer throughout (ideally that of the DSL) that will not be used by young people and if necessary can be taken off site by the police should the need arise.**
- It is important that the relevant staff 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 retained as evidence (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the investigating staff will need to judge whether or not this concern has substance. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Referral to the Police for their involvement and/or action

If content being reviewed includes images of Child abuse then all monitoring should be halted and the matter 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
- other criminal conduct, activity or materials

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. All records and documentation should be retained by the School for evidence and reference purposes.