Saint Nathaniel's Academy

Online Safety Policy

Date last reviewed: February 2024

Reviewed by: RPatrick.

Date for next review: February 2026

'With God all things are possible' Matthew 19:26

Online Safety Policy

Scope of the Policy

Online Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. The policy will operate in conjunction with other policies including those for student Behaviour, Anti-Bullying, Curriculum, Data Protection and Safeguarding. This policy applies to all members of the academy community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy ICT systems, both in and out of the academy.

What is Online Safety?

Online Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

End to End Online Safety

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students, encouraged by education and made explicit through published policies.
- Sound implementation of Online Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Schools Broadband with effective filtering systems.
- National Education Network standards and specifications.

Legislation and Statutory Guidance

This policy is based on the Department for Education’s statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department’s guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils’ electronic devices where they believe there is a ‘good reason’ to do so. The policy also takes into account the National Curriculum computing
programmes of study.

It is the duty of the school to ensure that every child and young person in its care is safe. The same ‘staying safe’ outcomes and principles outlined in the Every Child Matters agenda apply equally to the ‘virtual’ or digital world. The Keeping Children safe in Education 2021 document sets out the legal duties that must be followed to safeguard and promote the welfare of children and young people under the age of 18 in schools and refers to online safety. This expectation also applies to any voluntary, statutory and community organisations that make use of the school’s ICT facilities and digital technologies.

Intent

- To ensure that all members of our academy community understand and are committed to promoting respectful and responsible internet use.
- To ensure that staff and pupils are aware of the benefits and risks associated with internet use and the use of social media.
- To ensure that all necessary measures are in place to safeguard all.
- To ensure that pupils feel safe and secure and are aware of how to keep themselves safe online.
- To ensure that all members are aware of their responsibilities to safeguard themselves and others when accessing the internet and engaging in online activities.

Reviewing the Online Safety policy

The Online Safety Policy relates to other policies including those for ICT, bullying and child protection (safeguarding). The ICT curriculum coordinator will also act as Online Safety coordinator. The Online Safety Policy and its implementation will be reviewed regularly.

Online Safety Audit – Saint Nathaniel's Academy

Date of latest update: June 2022
The updated policy will be shared with the Local Governing Committee: June 2022
The Policy is available for staff and parents at: Policies | saint-nathaniels (saintnathaniels.org.uk)
The Designated Child Protection Coordinator is: Miss L Clarke (Vice Principal / Inclusion Lead)
The Online Safety Coordinator is: Mr M. Field (Online Safety Lead)

Has Online Safety training been provided for staff?	[✓ Y]/N
Has Online Safety training been coherently planned and delivered for pupils? –***ongoing across all year groups and embedded in the Curriculum.***	[✓ Y]/N
Do all staff sign an ICT Code of Conduct on appointment?	[✓ Y]/N
Do parents sign and return an agreement that their child will comply with the school Online Safety Rules?	[✓ Y]/N
Have school Online Safety Rules been set with pupils?	[✓ Y]/N
Are these Rules displayed in all rooms with computers?	[✓ Y]/N
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access (e.g. Schools Broadband).	[✓ Y]/N
Is personal data collected, stored and used according to the principles of the General Data Protection Regulation 2018?	[✓ Y]/N
Do all school computers have Online Safety text monitoring software (Forensic) installed?	[✓ Y]/N
Has the school filtering policy been approved by SMT? (N/A unless school has taken over responsibility)	[✓ Y]/N
If the school has taken responsibility for its own web filtering, have appropriate members of staff attended training on the filtering system and are appropriate procedures in place?	[✓ Y]/N

Teaching and learning

Technology is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

In 2021 the school moved to 1:1 iPad implementation with the children. The iPad is a tool for teaching and learning. Through the use of Apple Classroom the staff can monitor the individual use of each iPad in their class. Through the app they can also safely navigate and lock children in and out of a variety of apps and websites. Staff are also aware that, if needed, they can lock iPads in order to check history and usage of each individual pupil. The use of Apple Classroom, Apple Manager and Jamf will further enhance our monitoring and E-Safety procedures.

Keeping children safe using iPads

- Staff are aware that the iPad is a tool to enhance teaching and learning through feedback and creativity.
- Staff understand that too much screen time is not good for the children.
- ICT technician (Mr S. Robinshaw) to manage the iPads using Apple School Manager
- Computing Lead (Mr M. Field) also has access to this system and Jamf which will enable and notify if children are misusing iPads.
- Internet safety filters applied to all pupil iPads.
- Staff trained on use of Apple Classroom which displays a live feed of children's screens to ensure safe use.
- Staff to 'Navigate' and 'Lock' pupil iPads when appropriate.
- If children do misuse the iPad, they will receive a ban (based on severity of incident) and alternative resources to be made available in the classroom.
- Outside agency Apple school support available through GBM and an Apple Specialist teacher (Ricky Brown).
- If the school decides to allow children to use iPads at home, parents will need to attend a meeting in school to discuss responsible use of devices.
- Parents will sign a declaration accepting responsibility of use of the iPad when it is at home.

Why are new technologies and Internet use important?

- The internet is an essential element in 21st century life for education, business and social interaction.
- The academy has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The purpose of internet use in school is to raise educational standards, to promote pupil achievement and to support the professional work of staff.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school has a duty to provide students with quality Internet access as part of their learning experience.

- Pupils use the Internet widely outside of school and will need to learn how to evaluate internet information and to take responsibility for their own safety and security.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include internet usage monitoring and web filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities and to raise attainment and achievement. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils’ age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of effective knowledge location, retrieval and evaluation.
- Pupils will be taught how to evaluate Internet content.
- The academy will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will be Taught How to Stay Safe Online

At Saint Nathaniel’s, we educate our very youngest learners about the importance of online safety as we recognise that pupils are accessing an online world both in the home and school environment.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

The safe use of social media and the internet will also be covered in other subjects where relevant. The academy will use assemblies to raise pupils’ awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Cyber-Bullying

The rapid development of and widespread access to technology has provided a new medium for ‘virtual bullying’, which can occur in and outside school. Cyber-bullying is a different form of bullying which can happen beyond the school day into home and private space, with a potentially bigger audience, and more accessories as people forward on content. The

importance of respectful online communications is explicitly taught and all pupils and parents are aware of our expectations.
The school will take all reasonable precautions to ensure against cyber-bullying whilst pupils are in its care. However, due to the global and connected nature of new technologies, it is not possible to guarantee that inappropriate use via a school computer will not occur. Neither the school, nor Stoke-on-Trent City Council, can accept liability for inappropriate use, or any consequences resulting outside of school.

• The school will proactively engage with pupils in preventing cyber-bullying by:
Understanding and talking about cyber-bullying, e.g. inappropriate use of e-mail, text messages;

- Keeping existing policies and practices up-to-date with new technologies;
- Ensuring easy and comfortable procedures for reporting;
- Promoting the positive use of technology;
- Evaluating the impact of prevention activities.
- Pupils, parents, staff and governors will all be made aware of the consequences of cyber-bullying.
- Parents will be provided with an opportunity to find out more about cyber-bullying through: session for parents, NSPCC support guidance, Know It All parents’ and other outside agency support.

How will cyber-bullying reports/issues be handled?
Records of any incidents of cyber-bullying will be kept and will be used to help to monitor the effectiveness of the school’s prevention activities. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risk will be reviewed regularly.

- Complaints of cyber-bullying will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head of School. Evidence of offending messages, pictures or online conversations will be kept, in order to demonstrate to others what is happening. It can be used by the school, internet service provider, mobile phone company, or the police, to investigate the cyber-bullying.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

Sanctions within the school discipline policy include:

- ○ Interview/counselling by the class teacher;
- ○ Informing parents or carers;
- ○ Removal of Internet/computer access for a period of time or banning of mobile phones in school

Prevent: Radicalisation and Extremism
Saint Nathanial's Academy takes an active role in protecting pupils from the risks of extremism and radicalisation. Keeping children safe from risks posed by terrorist exploitation of social media is approached in the same way as safeguarding children from any other online abuse. In the same way teachers are vigilant about signs of possible physical or emotional abuse, we are vigilant about any signs of radicalisation or extremism in any of our pupils. We follow the same safeguarding procedure to ensure all children in our care are well looked after.
For more information on Prevent, Radicalisation and Extremism please follow the link on our website on the Online Safety page.

Managing Internet Access

Information system security.
School ICT systems capacity and security will be reviewed regularly.
Virus protection will be updated regularly.
Security strategies will be discussed within Saint Bart's Trust.

E-mail
(Currently blocked and only opened if Teacher requests e.g. covering within the curriculum)
Pupils may only use approved e-mail accounts/messaging systems on the school system.
Pupils must immediately tell a teacher if they receive offensive e-mail or messages.
Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published content and the school learning platform
The contact details on the Web site must be the school address, e-mail and telephone number.
Staff or pupils' personal information will not be published.

Publishing pupils' images and work
Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. (No children's names to be used).
Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
Written permission from parents or carers will be obtained before photographs of pupils or pupils' work are published on the school Web site. This is done on entry to school.
No photographs of Looked after Children should be displayed.

Social networking and personal publishing

The school will block/filter access to social networking sites.
Newsgroups will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Managing filtering

The school will work with the LA, Stoke on Trent Safeguarding board and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Coordinator. (Mr Field who will directly report to SLT and block accordingly).
The ICT co-ordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Managing remote teaching/video-conferencing

The equipment and network

- Full IP videoconferencing will use the national educational or the schools' broadband network to ensure quality of service and security.
- All videoconferencing equipment in the school/classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact information will not be put on the school website.
- School videoconferencing equipment will not be taken off school premises without permission, since use over a non-educational network (e.g. the internet) cannot be monitored or controlled.

Users

- Pupils will ask permission from the supervising teacher before making or answering a videoconference call if this is available in the near future.
- Videoconferencing will be supervised appropriately for the pupils' age.
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.

- Only key administrators will be given access to the videoconferencing system, web or other remote control page available on larger systems.
- Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.
- When delivering Zoom lessons staff will always team teach in order to monitor safe and appropriate use of technology.

Content

- When recording a videoconference lesson, written permission will be sought by all sites and participants. The reason for the recording is given and the recording of videoconference is clear to all parties at the start of the conference.
- Recorded material will be stored securely.
- If third-party materials are to be included, recordings will be checked that they are acceptable to avoid infringing the third party intellectual property rights.
- Dialogue will be established with other conference participants before taking part in a videoconference. If it is a non school site it is checked that they are delivering material that is appropriate for the class.

Pupils using devices for home learning

If it is decided that iPads are to be used at home by children to access home learning:

- Staff will provide feedback on work completed and monitor the safe use of the iPads.
- IPads will be managed through Jamf (M. Field) and set to lock at 7pm to reduce screen time and the risk of inappropriate use.
- Agreement signed by parents clearly shows the SMART Online Safety guidelines.
- Home learning policy will follow SBMAT Acceptable Use Policy and Remote Learning.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions (ICT co-ordinator to share links to policies with staff)

Authorising Internet access

- All staff must read and adhere to the acceptable use policy before using any school ICT resource.
- Access to the Internet will be by supervised access to specific, approved on-line materials.
- All staff must read and understand the related computing policies (see Related policies).

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor local authority can accept liability for the material accessed, or any consequences of Internet access. If unsuitable material appears, the Online Safety coordinator & SLT will be informed so that relevant filtering can be completed.

The school will audit ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective.

Handling Online Safety complaints

Complaints of Internet misuse will be dealt with by the class teacher and where necessary a senior member of staff.

- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils are expected to work in partnership with staff to resolve issues or concerns.

Sanctions within the school behaviour policy will include:

o interview/counselling by Inclusion/SLT;
o informing parents or carers;
o removal or restriction of Internet or computer access for a period.

- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Community use of the Internet

External organisations using the school's ICT facilities must adhere to the Online Safety policy. Internet use by staff and children is actively monitored.

Communicating the Online Safety Policy

Introducing the Online Safety policy to pupils

- Online Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year and throughout the year as part of computing and PHSE sessions.
- Pupils will be informed that network and Internet use will be monitored.
- An Online Safety training programme will be introduced to raise the awareness and the importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.
- An Online Safety module will be included in the PSHE/RSE and Computing programmes covering both school and home use.

Staff and the Online Safety policy

- All staff will be given the School Online Safety Policy and its application and importance explained.
- All staff will be informed that all computer and Internet use will be monitored. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on the school Online Safety Policy will be provided as required.

- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. In addition, all staff members will revisit or review this training as part of our annual safeguarding updates.

Enlisting parents' support

- Parents' attention will be drawn to the school's Online Safety Policy in relevant newsletters, prospectus, the school website and through parent workshops.

- A guide to Responsible Internet Use is also available on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Online Safety updates will be shared on both Class Dojo and other school social media to keep parents updated on relevant information.

Mobile Technology Device Policy

- All devices that have access to a) the internet and b) the school network must be password protected. The purpose of this is to prevent data loss and protect pupils and staff.

Staff passwords

- Staff each have their own username and unique password.
- Staff generate their own password and understand that they must not share passwords. Records of staff passwords are not stored but the passwords can be overwritten or reset by the network administrator
- Staff are expected to change their passwords at least annually to ensure that they remain secure.
- Staff with access to sensitive data change their passwords every term.

Pupil passwords

- Each pupil has their own username and password for use on Purple Mash and other software.
- Staff record the pupil use of numbered laptops and iPads in order to track any un-safe behaviour online or misuse of ICT software and equipment.

USB device password

- USB devices are encrypted and password protected. The encryption password is universal.
- Hard drive encryption password
- Laptop hard drives are encrypted and password protected. The encryption password is universal.

Please also refer to SBMAT Acceptable Use Policy; Learners and Staff

Personal mobile devices – staff and visitors

- Staff and visitors are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office.
- Staff and visitors should have their devices on silent or switched off and out of sight (e.g. in a drawer, handbag) during class time.
- Mobile phones should not be used in a space where children are present (e.g. classroom, playground).
- Use of devices (including receiving/sending texts and emails) should be limited to non contact time when no children are present e.g. in office areas, staff room, empty classrooms.

- Staff and visitors are not permitted to take photos or recordings or use any recording software with their personal devices.
- Devices connected to the internet are subject to the same web filtering as any other devices.
- Should there be exceptional circumstances (e.g. acutely sick relative), then staff and visitors should make the Principal and office staff aware of this so messages can be relayed promptly.
- Staff and visitors should report any usage of mobile devices that causes them concern to the Principal.
- All staff and visitors must password protect their mobile device.

Personal mobile devices – pupils

- Pupils to only have phones when permission is granted from the school and parents in circumstances such as Year 6 children walking home alone.
- Phones must be switched off during the school day.
- Emergency contact to be made through the school office
- Children are not permitted to take photos or recordings or use any recording software with their personal devices.
- Devices connected to the internet are subject to the same web filtering as any other devices.

School owned mobile devices – staff

- All mobile devices including USB sticks must be password protected to prevent data loss
- All mobile devices must be protected by the school's web filtering system
- Passwords to devices must not be shared with anyone who is not employed by the school.

School owned mobile devices – pupils

- All mobile devices must be protected by the school's web filtering system
- Devices intended for pupil use must not leave the school
- Pupils must access mobile devices using pupil user accounts only
- Pupil mobile device user accounts must block any attempted file downloads, block

access to the computer's system files, block access to the control panel, block access to the command prompt and only map the student network drive.

Miscellaneous

- WIFI access code to be held by the ICT technicians, Principal, Vice Principals and Computing Lead only.

Related policies & Documents

There are a number of other policies at Saint Nathaniel's Academy which relate to the topics mentioned above. It is important that you read and fully understand the polices below which can be found on the Saint Nathaniel's Academy staff drive. If you have any questions about this policy or any other policies please ask Mr Field.

- SBMAT Acceptable Use Policy - Policies | saint-nathaniels (saintnathaniels.org.uk)
- Data Protection Policy - Policies | saint-nathaniels (saintnathaniels.org.uk)
- Social Media Policy
- Filtering Policy
- Parent / Carer acceptable use policy
- Use of digital and video images
- Pupil iRules
- Computing policy

I have read and understood the Online Safety policy and the above policies.

Name ________________________ Date ___________________________

Social Media Policy

Social media (e.g. Facebook, Twitter, Tik Tok, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by *the school*, its staff, parents, carers and children.

Scope

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education
- *Defines the monitoring of public social media activity pertaining to the school*

The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. 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.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Organisational control

Roles & Responsibilities

SLT

- Facilitating training and guidance on Social Media use.
- Developing and implementing the Social Media policy
- Taking a lead role in investigating any reported incidents.
- Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.

Staff

- Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
- Attending appropriate training
- Regularly monitoring, updating and managing content he/she has posted via school accounts
- Adding an appropriate disclaimer to personal accounts when naming the school
- Plan, and deliver lessons using 'Progression in Online Safety' from Purple Mash and Project Evolve
- Teach online safety as part of RSE/PHSE lessons.

Managing accounts

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, eg a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:

- The aim of the account
- The intended audience

- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

- **School accounts must be monitored regularly and frequently**. Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of personal social media by staff while at work is prohibited.
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

- The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:
- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, eg. Facebook)

Use of images

- School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.
  - **Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy**. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
  - **Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts**
  - Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
  - If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

Staff

- Personal communications are those made via a personal social media accounts. 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.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *The school permits reasonable and appropriate access to private social media sites.*

Pupil/Students

- **Staff are not permitted to follow or engage with current or prior pupils/students of the school on any personal social media network account.**
- The school's education programme should enable the pupils/students to be safe and responsible users of social media.
- Pupils/students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts

- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem?

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don’t make comments, post content or link to materials that will bring the school into disrepute
- Don’t publish confidential or commercially sensitive material
- Don’t breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don’t link to, embed or add potentially inappropriate content
- Don’t post derogatory, defamatory, offensive, harassing or discriminatory content
- Don’t use social media to air internal grievances

Saint Nathaniel’s Academy Internet Filtering Policy

SSID - Jbaskeyfield
All internet use on all devices at Saint Nathaniel’s Academy is filtered. The firewall is controlled by the ISP (internet service provider) School’s Broadband.

SSID Password
Access to the WIFI is protected by a password. The password is held by the IT Technician and IT co coordinator. The password is not to be given out for any reason.

Connecting a new device
Devices that are not already connected to the network are to be connected by the IT Technician.

Filtering levels
At Saint Nathaniel’s Academy there are three levels of web filtering which are controlled and administrated by the IT Technician.

1. Allow all (used by network administrators, SLT and safeguarding staff)
2. Staff web (used by staff not listed above)
3. Pupil web (used by pupils)

Allow all – Free internet use.
Pupil web – Highly restricted web use. Blocks sites and searches based on key words/phrases as well as by category.
Staff web – Works the same as pupil web but with less restrictions allowing staff to search for resources more freely.

Safety net

Filtering levels are assigned to a person based on their username. If a device does not require a username such as a tablet or mobile phone or the username is not recognised by the filtering system, the device is automatically assigned the pupil web filter level.

Globally blocked / globally allowed

We also have the option to add a site to a globally blocked or globally allowed list.
If a member of staff finds a site which they feel should be blocked which isn't, they must report it to the IT Technician who will add it to the globally blocked list.
If a member of staff needs access to a blocked site, they must report it to the IT Technician.
The IT Technician is to review the sites content and add it to the globally allowed list if the site is appropriate.

Reporting

A report is run once a month to show any attempts to access any blocked websites and also blocked search queries. The report shows who has tried to access the site and at what time.
There is also the option to run full internet usage reports based on username if required.
IT technicians will share the report with M Field & L Clarke.

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students / pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users. A copy of the Student / Pupil iRules is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name		Student / Pupil Name	

As the parent / carer of the above *pupils*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

Either: (KS2 and above)

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

Or: (KS1)

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, Online Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

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

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

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

Signed

Date

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

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

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

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

Digital / Video Images Permission Form

Parent / Carers Name

Pupil Name

As the parent / carer of the above *student / pupil*, I agree to the school taking and using digital / video images of my child / children. I understand

Yes / No

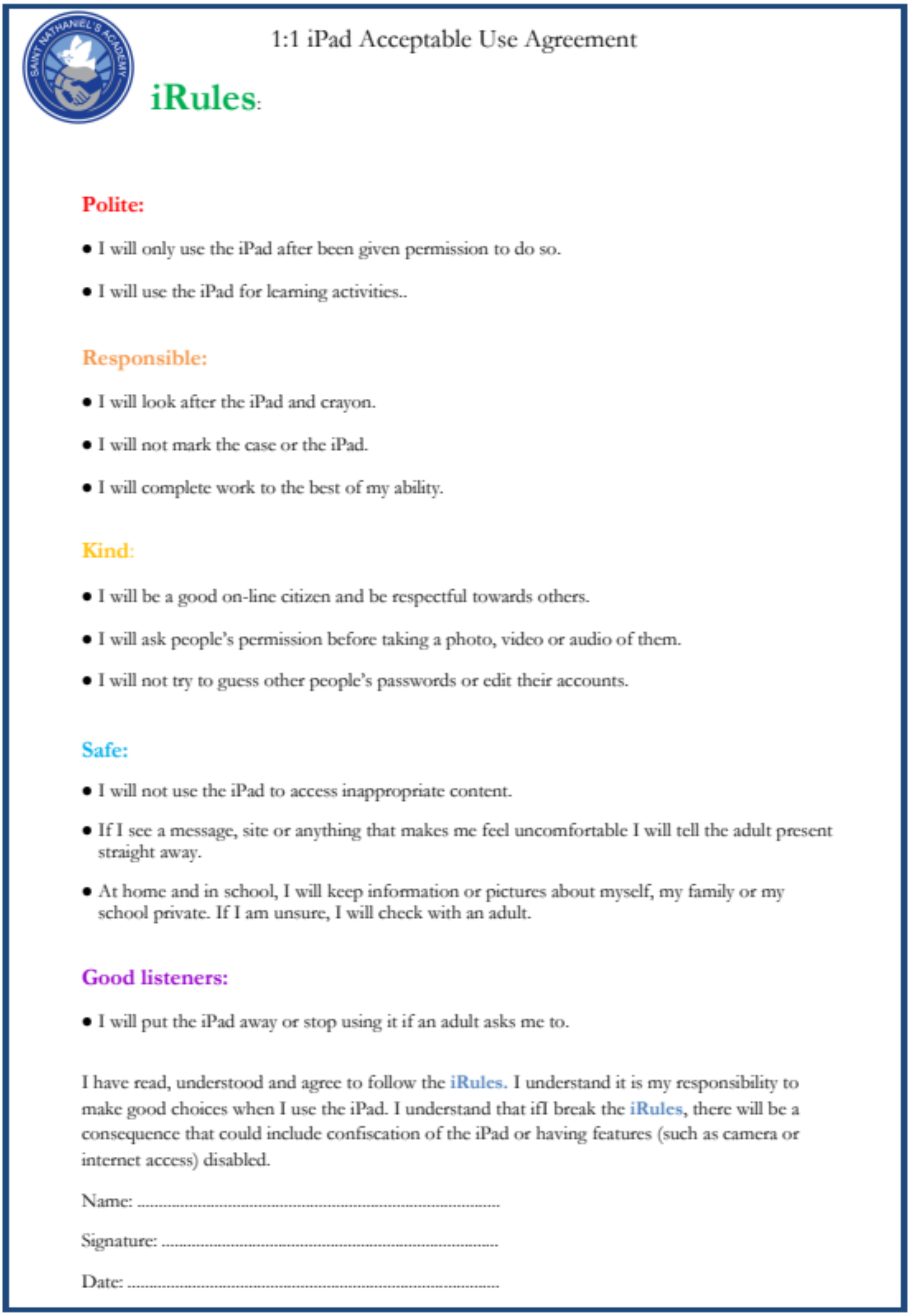
that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Yes / No

Signed

Date



1:1 iPad Acceptable Use Agreement

iRules:

Polite:

- I will only use the iPad after been given permission to do so.
- I will use the iPad for learning activities..

Responsible:

- I will look after the iPad and crayon.
- I will not mark the case or the iPad.
- I will complete work to the best of my ability.

Kind:

- I will be a good on-line citizen and be respectful towards others.
- I will ask people’s permission before taking a photo, video or audio of them.
- I will not try to guess other people’s passwords or edit their accounts.

Safe:

- I will not use the iPad to access inappropriate content.
- If I see a message, site or anything that makes me feel uncomfortable I will tell the adult present straight away.
- At home and in school, I will keep information or pictures about myself, my family or my school private. If I am unsure, I will check with an adult.

Good listeners:

- I will put the iPad away or stop using it if an adult asks me to.

I have read, understood and agree to follow the iRules. I understand it is my responsibility to make good choices when I use the iPad. I understand that ifI break the iRules, there will be a consequence that could include confiscation of the iPad or having features (such as camera or internet access) disabled.

Name: ....

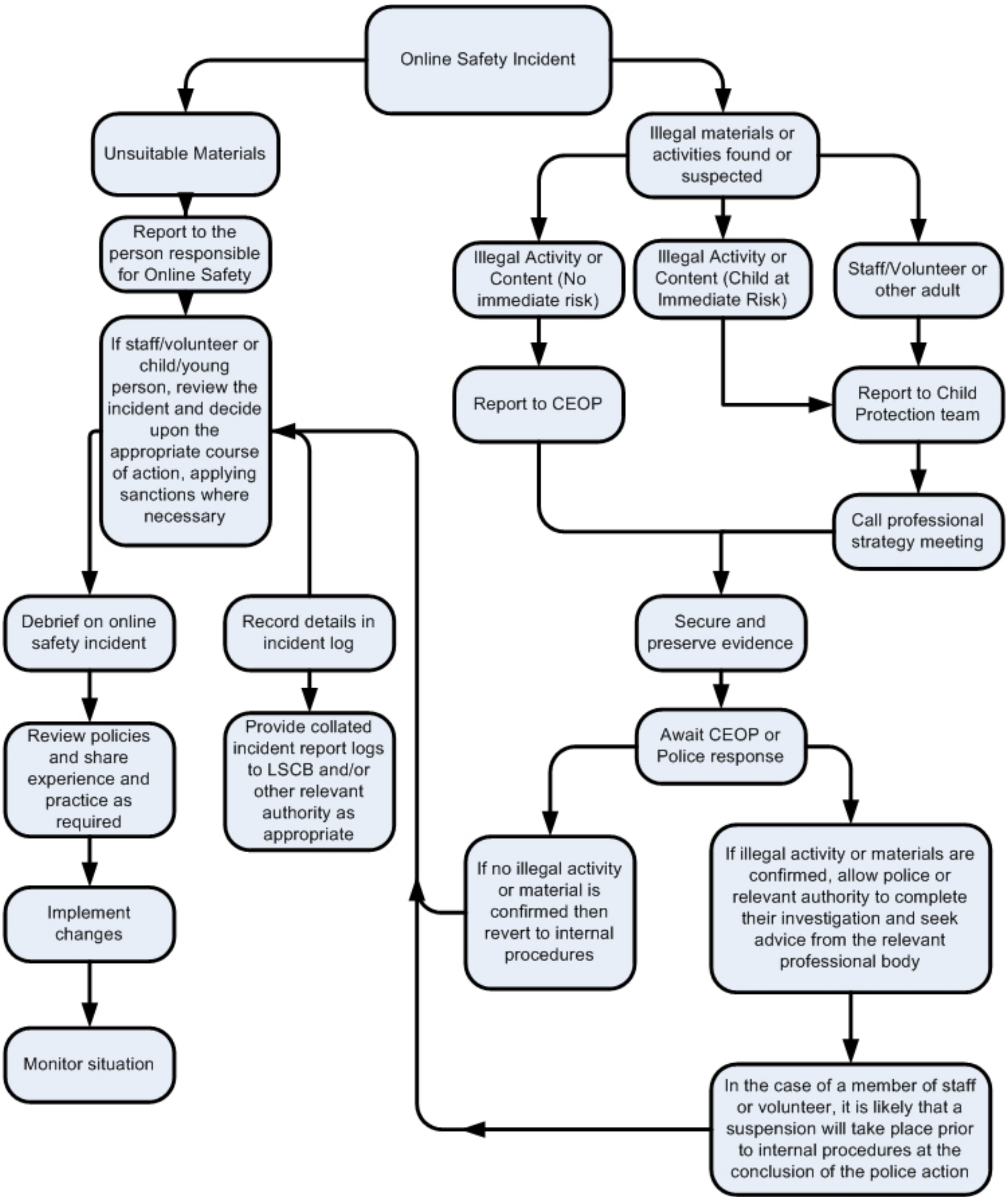
Signature: ....

Date: ....

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key Online Safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Networked favourites Ikeepbookmarks.com
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Yahooligans CBBC Search Kidsclick Kiddle (Google kids)
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	School Net Global E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites for feedback.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted. Pupils should be encouraged to report any inappropriate comments.	Making the News Podcasts Video/Film Photograph
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News SuperClubs Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within blogs, chat rooms or online forums.	Only blogs/chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Skype Zoom FlashMeeting Purple Mash
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype Zoom FlashMeeting National Archives "On-Line" Global Leap National History Museum Imperial War Museum

Responding to incidents of misuse – flow chart


Online Safety Incident
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
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
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

Acknowledgement:

SWGF templates were used to assist the writing of this policy. (http://swgfl.org.uk/products-services/esafety/resources/onlinOnline Safety-policy-templates)