INTERNET SAFETY POLICY FOR GREAT MARSDEN ST.JOHN'S PRIMARY – A Church of England Academy

This Internet Safety policy was approved by the Local Governing Committee on	
The implementation of this Internet Safety policy will be monitored by the:	*Michaela Underwood (DSL)* *Elaine Walsh (Dep DSL)* *Computing Lead* *Nicole Ingham (Admin Officer and Social Media Lead)* *Matt McIver* *LGC*
Monitoring will take place at regular intervals:	*Annually*
The Local Governing Committee will receive a report on the implementation of the Internet Safety Policy	*Three times per year via the Head teachers report to Governors.*
The Internet 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 Internet Safety or incidents that have taken place. The next anticipated review date will be:	*October 2023*
Should serious Internet Safety incidents take place, the following external persons / agencies should be informed:	*Police* *LADO* *Trust CEO and COO*

Our Vision

Our children will experience love, respect, faith and success as unique individuals within our school community and the wider world, now and in the future.

Our Mission

"We ask that Christ will live in our hearts through faith making us rooted and grounded in LOVE."

Development / Monitoring / Review of this Policy

This Internet Safety policy has been developed by

- Headteacher
- Internet Safety Officer who is also the DSL
- Staff – including Teachers, Support Staff, Technical staff
- Local Governing Committee Representative

Schedule for Development / Monitoring / Review

The policy will be monitored by:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering which is provided by Lightspeed.
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students / pupils
    - parents / carers
    - staff

Scope of the Policy

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

In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The academy will deal with such incidents using guidance from this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Internet Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the Internet Safety roles and responsibilities of individuals and groups within the academy:

Local Governing Committee:

Governors are responsible for the approval of the Internet Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about Internet Safety incidents and monitoring reports. A member of the Local Governing Committee has the role of the Internet Safety Governor. This is a role combined with that of Safeguarding Governor.

Head teacher and Senior Leaders:

- The Head teacher has a duty of care for ensuring the safety (including Internet Safety) of members of the school community, though the day to day responsibility for Internet Safety will be the responsibility of the Head teacher in her role as DSL.
- The Head teacher and Senior Leadership Team are aware of the procedures to be followed in the event of a serious Internet Safety allegation being made against a member of staff. (See flow chart on dealing with Internet Safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Cidari MAT disciplinary procedures.
- The Head teacher and Senior Leaders ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Internet Safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles.

Internet Safety Lead/DSL – both roles sit with the Head teacher:

- Takes day to day responsibility for Internet Safety issues and has a leading role in establishing and reviewing the school Internet Safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Internet Safety incident taking place.
- Provides training and advice for staff
- Liaises with Cidari Mat and LA where applicable.
- Liaises with school technical staff
- Receives reports of Internet Safety incidents and creates a log of incidents to inform future Internet Safety developments,
- Meets regularly with Internet Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- Reports regularly to Senior Leadership Team

Computing Lead and Technical staff:

The Computing Lead and Technical Staff will ensure:

- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the academy meets required Internet Safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the Filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with Internet Safety technical information in order to effectively carry out their Internet Safety role and to inform and update others as relevant
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher who is also DSL and has overarching responsibility for Internet Safety.
- that monitoring software / systems are implemented and updated as agreed in school / academy policies

Teaching and Support Staff:

Are responsible for ensuring that:

- they have an up to date awareness of Internet Safety matters and of the current Internet Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Computing Lead and Headteacher/Internet Safety Lead for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- Internet Safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Internet Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, smart watches, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead and Deputy DSL:

Should be trained in Internet Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- sexting
- peer on peer abuse

Students / Pupils:

- are responsible for using the academy digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good Internet Safety practice when using digital technologies out of school and realise that the academy's Internet 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. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / and information about national / local Internet Safety campaigns / literature. Parents and carers will be encouraged to support the academy in promoting good Internet Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student / pupil records
- their children's personal devices in the school / academy (where this is allowed).

Policy Statements

Education –Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of pupils in Internet Safety is therefore an essential part of the academy's Internet Safety provision. Children and young people need the help and support of the school to recognise and avoid Internet Safety risks and build their resilience.

Internet Safety should be a focus in all areas of the curriculum and staff should reinforce Internet Safety messages across the curriculum. The Internet Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned Internet Safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Pupils should 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.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should 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.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside the academy.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons, where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

Many parents and carers have only a limited understanding of Internet Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site,
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites and publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community:

The academy will provide opportunities for the local community to gain from the academy's Internet Safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and Internet Safety
- Internet Safety messages targeted towards grandparents and other relatives as well as parents.
- The school / academy website will provide Internet Safety information for the wider community

Education & Training – Staff / Volunteers

It is essential that all staff receive Internet Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Internet Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the Internet Safety training needs of all staff will be carried out regularly.
- All new staff should receive Internet Safety training as part of their induction programme, ensuring that they fully understand the academy Internet Safety Policy and Acceptable Use Agreements.
- The Internet Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Internet Safety Policy and its updates will be presented to and discussed by staff.

- The Internet Safety Lead and Computing Lead will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in Internet Safety training / awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school / academy training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

The academy will be responsible for ensuring that the academy infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their Internet Safety responsibilities:

- Academy technical systems will be managed in ways that ensure that the school / academy meets recommended technical requirements. BT Lancashire and Dataspire are our partners in this.
- There will be regular reviews and audits of the safety and security of the academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to academy technical systems and devices.
- All adult users will be provided with a username and secure password by the Computing Lead/SAM/Technical Support who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every academic year. Class log-ons and passwords are used for children and the policy makes clear the associated risks.
- The "administrator" passwords for the academy ICT system, used by the Network Manager (or other person) must also be available to the Head teacher, SAM and Computing Lead and kept in a secure place.
- The Computing Lead in collaboration with the ICT Technician are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider – Lightspeed- 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 should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Academy technical staff and Computing Lead 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.
- An appropriate system is in place, described later in the Policy, for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- Appropriate security measures are in place, Lenovo, to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place, to be described, for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place, described later in the Policy, regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. As we are Cloud based this should be minimal.

Mobile Technologies

Mobile technology devices may be academy owned/provided or personally owned and might include: smartphone, smartwatch, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile / personal devices in a school context is educational. The Mobile Technologies Policy should be consistent with and interrelated to other relevant school policies including but not limited to the Internet Safety Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Internet Safety education programme.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber 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. The academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils 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.
- Written permission from parents or carers will be obtained before photographs of pupils 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 academy events for their own personal use (as such use is not covered by the Data Protection Act). General image making will not be permitted to safeguard those children whose parents do not wish their image to be used.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy 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 academy 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 students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection GDPR

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights

- Secure
- Only transferred to others with adequate protection.

The academy must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents

Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer confidential data using encryption, secure password protected devices and Google Drive.

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

- the data must password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies the academy considers the following as good practice:

- The official academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the academy policy, 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.
- Any digital communication between staff and students / pupils or parents / carers (email, social media, chat, blogs, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school / academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses will be used in all instances of educational use.
- Pupils should be taught about Internet Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school / academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the academy or Multi Academy Trust liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School / academy staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school / academy 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 academy.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school / academy social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts,
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school / academy disciplinary procedures

Personal Use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the academy 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 academy permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The academy's use of social media for professional purposes will be checked regularly by the Social Media Lead and Head teacher to ensure compliance with the school policies.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy and all other technical systems and reported to teh police.

Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in an academy context, either because of the age of the users or the nature of those activities.

The academy believes that the activities referred to in the following section would be inappropriate in an academy context and that users, as defined below, should not engage in these activities in / or outside the academy when using academy equipment or systems. The academy policy restricts usage as follows - the list is not exhaustive :

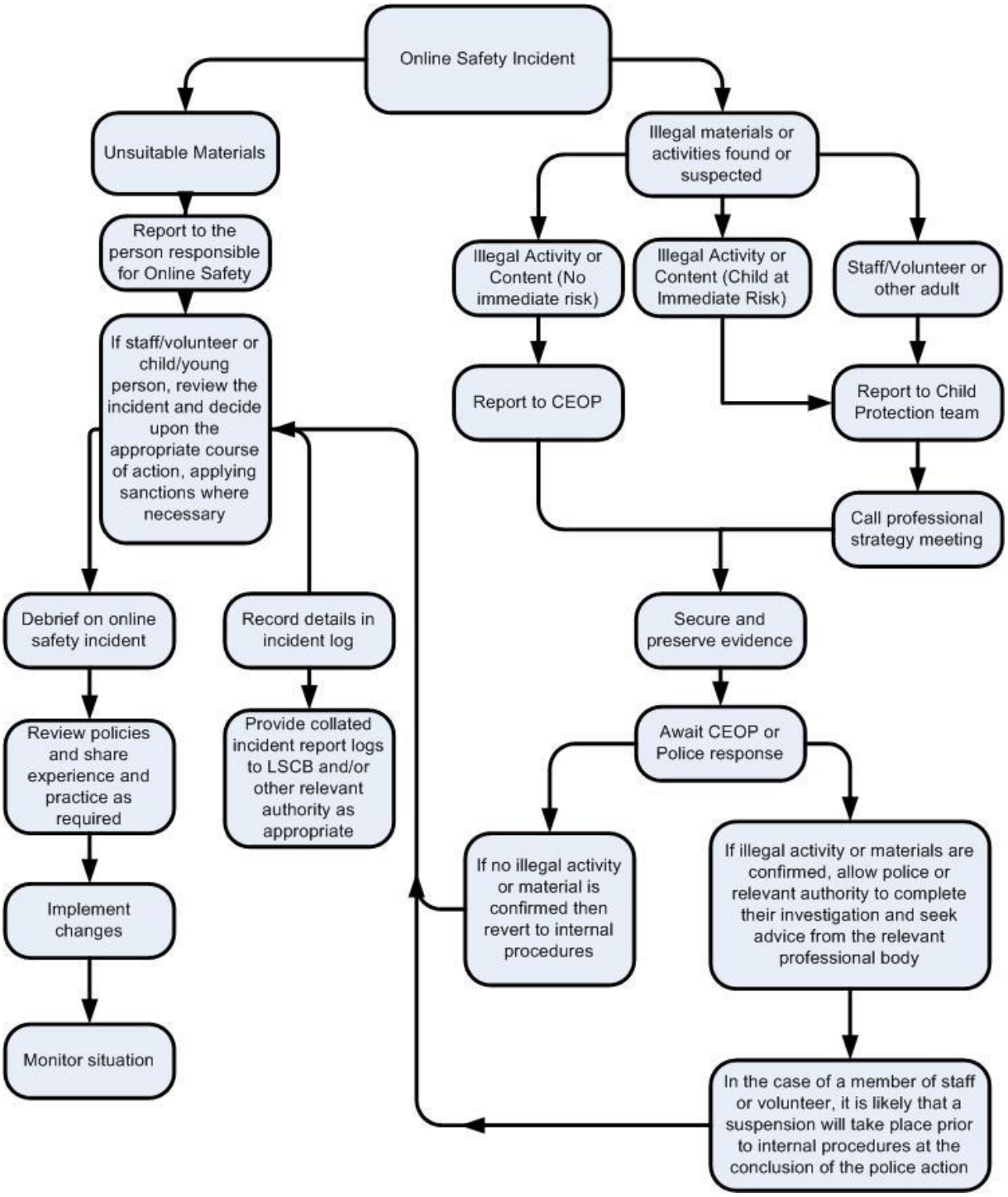
- Promotion of any kind of discrimination
- Threatening behaviour, including promotion of physical violence or mental harm
- Promotion of extremism or terrorism
- Using school systems to run a private business
- Unfair usage (downloading / uploading large files that hinders others in their use of the internet)
- On-line gambling

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to Internet Safety incidents and report immediately to the police.


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

Other Incidents

It is hoped that all members of the academy community will be responsible users of digital technologies, who understand and follow academy 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 / Cidari Multi Academy Trust.
    - 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
    - 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 academy 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.

Academy Actions & Sanctions

It is more likely that the academy 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 academy 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 as follows:

Actions by Pupils	Actions taken by Academy						
	Refer to Head teacher	Refer to Police	Refer to Computing Lead and technical support staff for action re filtering / security etc.	Informparents / carers	Removal of network / internet access rights	Warning	Further sanction in line with Behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X			X
Unauthorised use of non-educational sites during lessons				X		X	X
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X			X		X	X
Unauthorised / inappropriate use of social media / messaging apps / personal email	X		X	X		X	X
Unauthorised downloading or uploading of files	X		X				
Allowing others to access school / academy network by sharing username and passwords	X		X	X			X
Attempting to access or accessing the school / academy network, using another student's / pupil's account			X	X			X

Attempting to access or accessing the school / academy network, using the account of a member of staff	X		X	X			X
Corrupting or destroying the data of other users			X	X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X case by case	X	X			X
Continued infringements of the above, following previous warnings or sanctions	X		X	X	X		X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school	X			X			X
Using proxy sites or other means to subvert the school's / academy's filtering system	X		X	X			X
Accidentally accessing offensive or pornographic material and failing to report the incident	X		X	X			X
Deliberately accessing or trying to access offensive or pornographic material	X		X	X		X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X		X				

Staff Incidents	Actions taken by Academy						
	Refer to Headteacher	Refer to Academy Central Team	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action

	Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X				X
	Inappropriate personal use of the internet / social media / personal email	X	X		X	X		
	Unauthorised downloading or uploading of files	X	X		X	X		
	Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X			X	X		
	Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X		X	X		
	Deliberate actions to breach data protection or network security rules	X	X		X	X		
	Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X		X	X		
	Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X		X			X
	Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X		X			X
	Actions which could compromise the staff member's professional standing – CASE BY CASE	X	X		X	X	X	X
	Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	X	X		X	X		
	Using proxy sites or other means to subvert the school's / academy's filtering system	X	X		X	X		
	Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X		
	Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X		X	X
	Breaching copyright or licensing regulations	X	X			X		
	Continued infringements of the above, following previous warnings or sanctions	X	X					X

Policy reviewed October 2022

Appendices

Children's Safe Computing Agreement.

Keeping safe: stop, think, before you click!

Pupil name: _____

I have read the school 'rules for responsible Computing use'. My teacher has explained them to me.

I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.

This means I will use the computers, Internet, e-mail, online communities, digital cameras, video recorders, and other ICT in a safe and responsible way.

I understand that the school can check my computer files, and the Internet sites I visit, and that if they have any concerns about my safety, that they may contact my parent / carer.

Pupil's signature _____

Date: ___/ ___/ ___

Keeping safe: stop, think, before you click!

12 rules for responsible ICT use

These rules will keep everyone safe and help us to be fair to others.

These rules will keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only delete my own files.
- I will not look at other people's files without their permission.
- I will keep my logon and password secure.
- I will not bring files into school without permission.
- I will ask permission from a member of staff before using the Internet.
- I will only email people I know, or my teacher has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet or by e-mail or in a chat room.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.

Great Marsden St John's Primary School
A Church of England Academy

Use of Digital / Video Images – This is delivered to Parents via the Induction Pro Forma

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 cannot 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 own 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 include any other children, unless permission is given by that child's parent/carer.

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

---

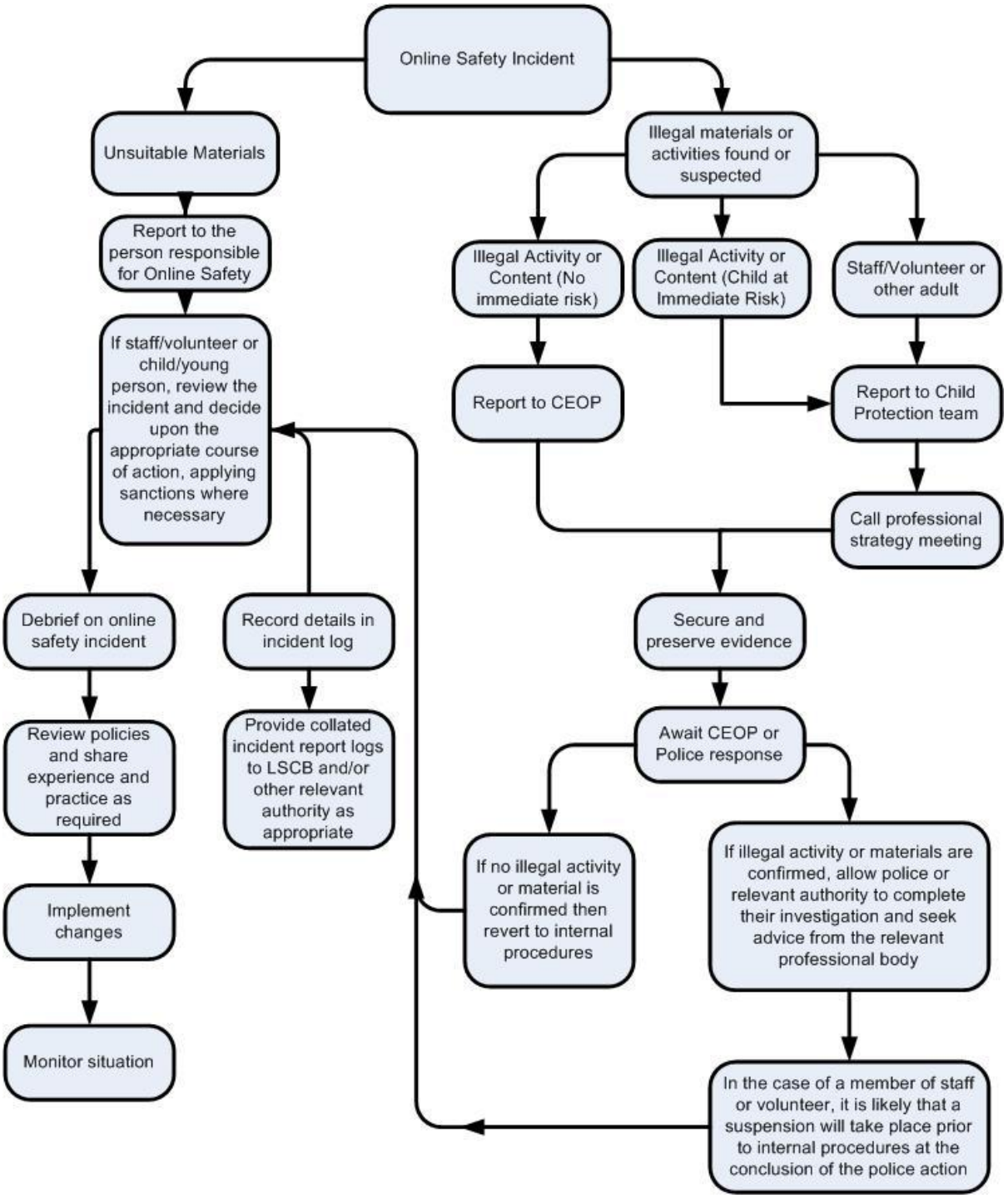
Digital / Video Images Permission Form

Parent / Carers Name	
Student / Pupil Name/s	

As the parent / carer of the above pupil I agree to the academy taking and using digital / video images of my child / children. I understand 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.	Yes / No
I agree that at school events I will abide by the guidelines set out above.	Yes / No

Signed	
Date	

Responding to incidents of misuse – flow chart



Record of reviewing devices / internet sites (responding to incidents of misuse)

Who was using: _____

Date: _____

Reason for investigation: _____

_____

_____

_____

Details of first reviewing person

Name: _____

Position: _____

Signature: _____

Details of second reviewing person

Name: _____

Position: _____

Signature: _____

Name and location of computer used for review (for web sites)

_____

_____

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken
