

# Computing & Online Safety Policy



July 2023



## E-Safeguarding Policy

### 1. Rationale

#### **Why Internet use is important**

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children 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.

#### **Internet use will enhance learning**

The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

### 2. Roles and Responsibilities

The following section outlines the Online Safety roles and responsibilities of individuals and groups within Newton Hill Community School.

#### **Governors:**

Governors are responsible for the approval of the Computing Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-safety Governor. The role of the E-safety Governor will include:

- Regular meetings with the Headteacher
- Regular monitoring of e-safety incident logs
- Regular monitoring of filtering/change control logs
- Reporting to relevant Governors

#### **Headteacher and Senior Leaders:**

The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse”).

The Headteacher/Senior Leadership Team are responsible for ensuring that the Computing Leader and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

The Headteacher/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the Computing Manager.

### **E-Safety Leader/Designated Safeguarding Lead:**

- leads on e-safety issues.
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff.
- liaises with relevant bodies.
- liaises with Trust-IT support.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- reports to Senior Leadership Team.

### **Computing Manager (Trust-IT):**

The Network Manager is responsible for ensuring:

- That Newton Hill Community School technical infrastructure is secure and is not open to misuse or malicious attack.
- That our school meets the required e-safety technical requirements and any Local Authority/other relevant body Computing Policy/Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the any networked environments and infrastructure are regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/ SLT/ Online Safety Coordinator.
- That monitoring software/systems are implemented and updated as agreed in the school policies.

### **3. Teaching and Support Staff:**

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current Computing Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Agreement.
- They report any suspected misuse or problem to the Headteacher/SLT/Computing Coordinator.
- All digital communications with students/parents/carers should be on a professional level and only carried out using official school systems.
- E-safety issues are embedded in all aspects of the curriculum and other activities.
- Students understand and follow the e-safety and acceptable use agreements.
- Students 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, cameras etc. in lessons and other activities (where allowed) and implement current policies with regard to these devices. This includes the removal of personal photographic devices that students may bring into school.

- in lessons where internet use is pre-planned students 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.

### **Child Protection/Designated Safeguarding Lead:**

The Child Protection/ Designated Safeguarding Lead should be trained in e-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.

### **Pupils:**

- Should understand the importance of adopting good e-safety practice when using digital technologies in or out of school.
- Are responsible for using 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.

### **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. Newton Hill Community will take every opportunity to help parents understand these issues through, newsletters, letters, website and information about national/local e-safety campaigns/literature. Parents and carers will be encouraged to support our school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- their children's personal devices.
- Understand that unacceptable or possibly libellous posts on own social medial accounts, concerning the school, staff or pupils will be always be challenged.

## **4. Policy Statements**

### **Education – students**

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of Newton Hill Community School's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

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

- A planned e-safety curriculum is provided as part of ICT/PHSE/other lessons and should be regularly revisited. E-safety forms part of every computer lesson.
- Key e-safety messages are reinforced as part of a planned programme of assemblies.
- Students 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.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students are taught to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- 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 students 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 students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

#### **Education – parents/carers:**

Parents/carers play an essential role in the education of their children and in the monitoring/regulation of their 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.

Newton Hill Community School 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.

#### **5. Technical – infrastructure/equipment, filtering and monitoring:**

The school uses a filtered internet service provided by a Netsweeper. The filter will stop most unsuitable searches or content being found (this includes inappropriate games, images, websites and links to radicalisation and extremist content etc). Any internet searches that use words which are inappropriate are flagged by the filtering system and reported to the headteacher (Lead DSL), Computing lead (DSL) and computing technician. The log reports which device has been used to enter any inappropriate words. A child uses their unique pupil login to access a laptop and this identification is provided in the report. iPads do not require a pupil login so we have assigned each child to a specific iPad. We keep a weekly log of the dates when the class and children use the devices.

If staff or pupils discover an unsuitable site, it must be reported onto CPOMS which informs SLT and DSLs about the event. The school will report this to the appropriate agencies including the filtering provider and record onto the appropriate safeguarding forms in accordance with the safeguarding policy.

Newton Hill Community School will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- Newton Hill Community School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school's technical systems.
- All users will have clearly defined access rights to school systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- The school has provided enhanced/differentiated user-level filtering.
- Newton Hill Community School technical staff regularly monitor and record the activity of users on the school systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential incident/security breach to the relevant person, as agreed.
- An agreed policy is in place 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 regarding the extent of personal use that users are allowed on school devices.
- Users are not permitted to download and or install applications (including executable or similar types) on to a Newton Hill Community School device or whilst using the school's systems, without agreement from the IT department.
- Users may use the following types of removable media for the purposes detailed:
- CD/DVD – Playing original video material, original music and viewing data written to the media that is owned by the user (who has copyright ownership). The use of software written to writable versions of this media is strictly prohibited.

### **Information system security**

All school computers & laptops have FortiClient installed to protect the network from virus infections. FortiClient automatically updates and scans the computers.

### **Social networking and personal publishing**

- Use such sites with extreme caution, being aware of the nature of what you are publishing on-line in relation to your professional position. Do not publish any information online which you would not want your employer to see.
- Under no circumstances should school pupils or parents, be added as friends, unless known to you as a friend or relative prior to your appointment.
- Your role in school requires a high degree of professionalism and confidentiality.
- Any communications or content you publish that causes damage to the School, Local Authority, any of its employees or any third party's reputation may amount to misconduct or

gross misconduct to which the School and Local Authority Dismissal and Disciplinary Policies apply.

- Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.
- The Local Authority expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Any communications made in a professional capacity through social media must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring the School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
- using social media to bully another individual; or
- posting images that are discriminatory or offensive or links to such content.

### Managing emerging technologies

Device	Pupils	Staff
Mobile Phones	Not allowed – unless approved specifically for that child by SLT. Handed into staff at school. Phones turned off.	Staff allowed in line with code of conduct/Safeguarding Policy.
Taking photos or videos on school equipment	Pupils allowed supervised by an adult	Staff allowed
Use of hand held devices such as personal gaming consoles	Not allowed – only permitted occasions	Not allowed
Use of personal email addresses in school	Not allowed	Staff allowed on school owned laptops out of working hours if necessary.
Use of school email address for personal correspondence.	Not allowed	Not allowed.
Use of online chat rooms	Not allowed	Not allowed
Use of instant messaging services	Not allowed – only within school internal systems with monitored checks	As pupils
Use of blogs, wikis, podcasts or social networking sites	Not allowed – only within school internal systems with monitored checks	As pupils
Use of video conferencing or other online video meetings	Not allowed – apart from those set up by and supervised by staff	As pupils

School iPads	Allowed, but need to be monitored by adults and directed to specific apps.	Staff allowed, adhering to the school acceptable computing use agreement.
Apple/Smart watches	Not allowed	Staff allowed, adhering to the school acceptable computing use agreement.

## **6. Use of digital and video images:**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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. Newton Hill Community 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 students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

In accordance with guidance from the Information Commissioner's Office, parents/carers may be given permission to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images. If there are children present whose parent/guardian have denied photo permissions then it might be necessary to withdraw permission for any parent to take photos and videos at the event.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow Newton Hill Community School policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes without the permission of the head teacher.

Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Students must not take, use, share, publish or distribute images of others without their permission.

Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.



Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of students are published.

Staff must not publish or display photographs or videos of children without ensuring that permission has been granted. A full list of permissions is provided to each teacher.

Student's work can only be published with the permission of the student and parents or carers.

## **7. Data Protection:**

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

Staff will ensure they properly log off from any computer after accessing personal data.

Staff will not remove personal or sensitive data from the school premises without permission of the head teacher and without ensuring such data is kept secure.

Staff will not share pupil data with outside agencies without clearance or improvement from the GDPR manager/ headteacher.

## **8. Communications:**

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.

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

When using communication technologies, Newton Hill Community School considers the following as good practice:

- Pupils may only use approved e-mail accounts on the school system (Purplemash) and email usage should be supervised and monitored by a staff member.
- Users must immediately report 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 or parents/carers (email, chat, etc.) must be professional in tone and content. Communication between staff and parents should be limited to school hours only 8:00 am – 5:00 pm.
- Students should be taught about e-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 website and only official email addresses should be used to identify members of staff.

## **9. Social Media - Protecting Professional Identity:**

Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render Newton Hill Community School or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Newton Hill Community School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: 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.

Staff should ensure that:

- No reference should be made in social media to students, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- The school's use of social media for professional purposes will be checked regularly.

## **10. Appropriate and Inappropriate Use by Staff or Adults:**

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.

They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

## **11. In the Event of Inappropriate Use**

If a member of staff is believed to misuse the internet in an abusive or illegal manner, a report must be made to the Headteacher/Designated Safeguarding Lead immediately and then the Managing Allegations Procedure and the Safeguarding and Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

## **12. Appropriate and Inappropriate Use by Children or Young People:**

Acceptable Use Agreements detail how children and young people are expected to use the internet and other technologies within Newton Hill Community School, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The children, beginning with years 3 to 6, will study and sign the Acceptable Use Agreement together in class with discussion to ensure a full understanding of the document. Parents will

be able to access the document on the school website so that they can see what is expected of their child. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school/education setting or other establishment.

Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond school/education setting or other establishment.

### **13. In the Event of Inappropriate Use**

Should a child or young person be found to misuse the online facilities whilst at school, the following consequences should occur:

- Any child found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period of time.
- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.
- A record of inappropriate use of technology will be added to the E-Safety Incident Log which is maintained by the computing manager.

In the event that a child or young person accidentally accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action.

Children are taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

### **Use of Mobile Phones and social media**

Children are not permitted to use mobile phones whilst on school premises.

Many children, especially as they move into KS2 own mobile phones and use social media platforms. This has a potential to lead to problems including bullying and Sexual Violence Sexual Harassment (SVSH) safeguarding concerns (see safeguarding policy). Through PHSE, assemblies and class discussions children will receive instruction on online safety as well as using such platforms respectfully and responsibly.

There are occasions when mobile phones and social media will be used in a negative way by pupils, which can lead to harm and embarrassment to other pupils. Although this often

happens out of school hours, the school will investigate. Parents will be informed and if required external agencies (including the police) will be contacted.

Only those KS2 children who walk home from school may bring a mobile phone. This must be handed in to a staff member before school and returned at the end of the day. Phones must be switched off on school premises.

Children must not use or keep mobile phones on their person whilst in school.

### **Cyber Bullying**

Bullying and abuse through social media is an increasing problem in all areas of society. It is our aim to teach children how to make the right choices of how to deal with and what to do if cyber bullying becomes a problem. PHSE, RHSE & Computing programmes of study cover cyberbullying alongside whole school assemblies.

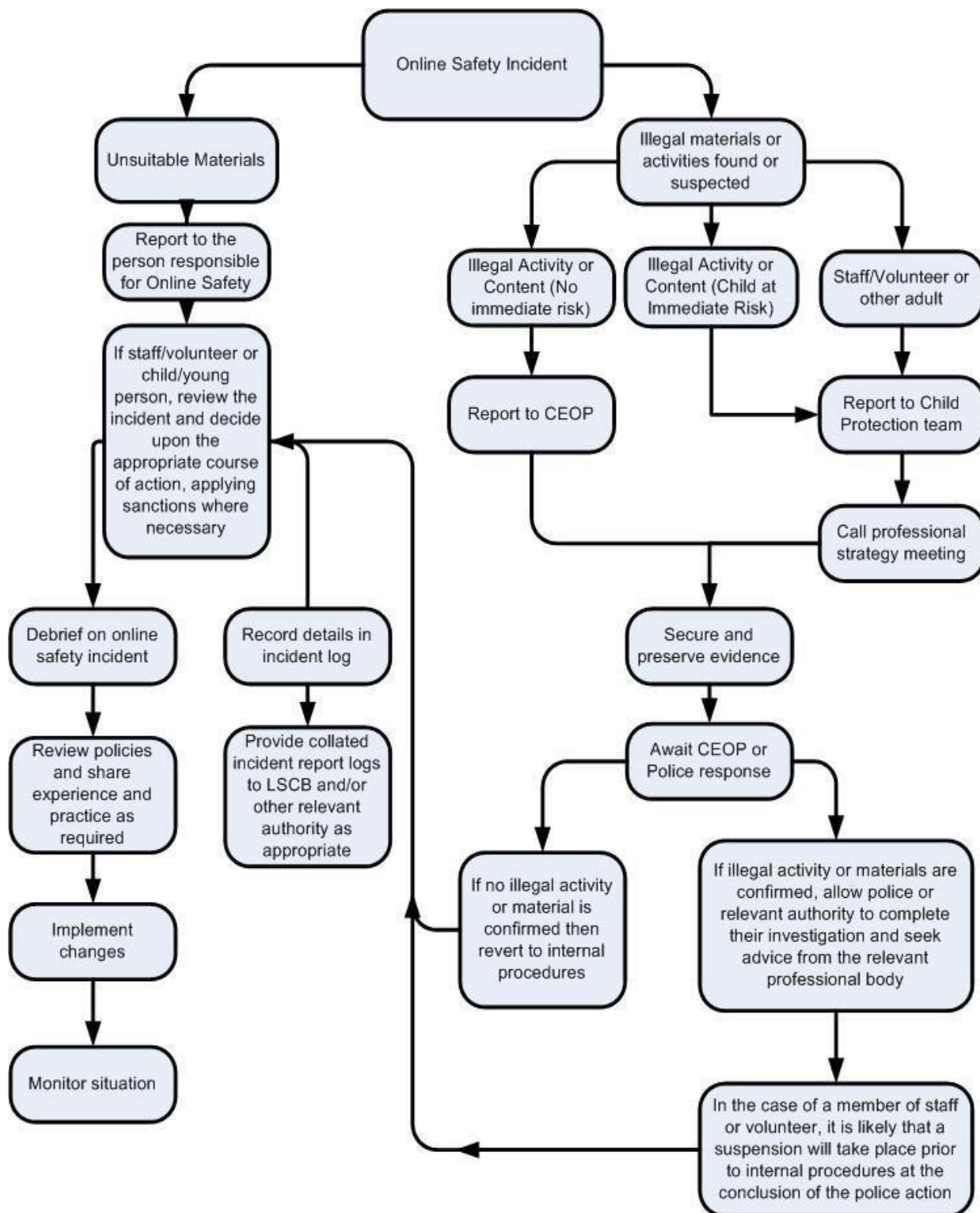
### **14. Responding to incidents of misuse:**

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 “In the Event of Inappropriate Use” above). See flow chart on the next page.

Complaints of internet misuse will be dealt with by a senior member of staff. Staff will Log any e-safety concerns on CPOMS. Any complaint about staff misuse must be referred to the head teacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures/ safeguarding policy.

### **15. 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 online safety incidents and report immediately to the police.



## 16. Other Incidents

It is hoped that all members of Newton Hill Community School will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

1. Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.

2. 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.
3. 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).
4. 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).
5. 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 of a national/local organisation (as relevant).
  - Police involvement and/or action.

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the Police would include:

- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

## **17. APPENDIX 1- Secure transfer of data and access out of school**

Newton Hill Community School recognises that personal data may be accessed by users out of the school, or transferred to other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should have secure remote access to the management information system or learning platform.

- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and Particular care should be taken if data is taken or transferred to another country, particularly outside Europe.
- Compliance with the General Data Protection Regulations should be at the core of all data storage, deletion and transfers to and from Newton Hill Community School.

## **APPENDIX 2- Staff/Volunteer Acceptable Use Agreement**

Newton Hill Community School  
ACCEPTABLE USE AGREEMENT  
(Staff/Volunteer)  
2023

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

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- Newton Hill Community School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

Newton Hill Community School will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

This policy applies to any device in the school. It applies across the whole network and includes Wi-Fi.

Newton Hill Community School carries out secure content inspection (SSL inspection). This means that when you access a site that uses techniques to secure the information between the website and yourself, Newton Hill Community School can read the information and remove inappropriate content or prevent access to the material. Excluded from this inspection are sites that contain sensitive financial information, including banks and payment systems.

Your activity on the internet is closely monitored by school, logs are kept of activity, whether on a school device or using your own device through the school Wi-Fi. These logs include who is accessing what material for how long from which device.

The school email system is provided for educational purposes, where required the school has the ability to access your school email for safeguarding purposes.

## Acceptable Use Policy Agreement

I understand that I must use Newton Hill Community School's ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that Newton Hill Community School will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to Newton Hill Community School ICT systems (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that Newton Hill Community School ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will be professional in my communications and actions when using Newton Hill Community School ICT systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images.
- I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the Newton Hill Community School website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in accordance with the school's policies
- I will only communicate with students and parents/carers using official systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

Newton Hill Community School has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs/laptops/mobile phones/USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.



- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in the school policies.
- I will not disable or cause any damage to the school equipment, or the equipment belonging to others.
- Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and restricted data must be held in lockable storage.
- I understand that Data Protection Policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that I am responsible for my actions in and out of Newton Hill Community School.
- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by Newton Hill Community School.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to follow these guidelines.

Staff/Volunteer Name: \_\_\_\_\_

Signed: \_\_\_\_\_

Date: \_\_\_\_\_

### **APPENDIX 3 – Pupil Acceptable Use Agreement**

These are the rules I agree to follow when using any digital technology:

- I will ask permission from a teacher before using ICT equipment and will use only my own login and password.
- To protect myself and other pupils, if I see anything I am unhappy with or receive messages I do not like, I will immediately tell a teacher or adult.
- I will not access other people's files or send pictures of anyone without their permission.
- I will not bring CDs or memory sticks into school unless I have permission and they have been checked to ensure that they are virus free.
- I will only e-mail people I know, or that my parent/teacher has approved and the messages I send will be polite and sensible.
- I will not give my home address or phone number, or arrange to meet someone I have met online.
- When I am using the internet to find information, I will check that the information is accurate as I understand that the work of others may not be truthful.
- Where work is protected by copyright, I will not try to download copies (including images, music and videos).
- I will not use my mobile phone in school for any reason.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- If I am involved in incidents of inappropriate behaviour that involve members of the school community (e.g. cyber-bullying, using images/information without permission), the school will take action according the Behaviour Policy.
- I understand that if I do not follow these rules I may not be allowed to use ICT in school and my parents/carers may be contacted.

I have read and understood these rules and agree to follow them:

Name of Pupil

Class

Signature

Date