



On line Safety Policy November 2021

'Learning to Live, Living to Learn'

Key Contact Personnel

Nominated Member of Leadership Staff Responsible for the policy: Tracey Jerome:
Headteacher

Designated Safeguarding Lead (s) Tracey Jerome: Headteacher Ellen Ranson McCabe:
Deputy Headteacher

Safeguarding Governor: Mrs Jane Davies

Technical Officer: Mr Carl Adams

Pastoral Assistant: Mrs Mandy Stanford

This online safety policy was approved by the Governing Body	
The implementation of this online safety policy will be monitored by the:	Senior Leaders and Goverbors
Monitoring will take place at regular intervals:	Policy to be reviewed annually
The Governing Body will receive a safeguarding report on the implementation of the online safety policy which will include anonymous details of online safety incidents at regular intervals:	FGB meetings
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	
Should serious online safety incidents take place, the following external persons/agencies should be informed:	LA Safeguarding Officer, On line safety officer, LADO, Police





On line Safety Policy November 2021

'Learning to Live, Living to Learn'

Learning to live! Living to Learn!

Inspired by our founder Mary Gibbon, we are a welcoming, nurturing community, providing the opportunity for each person to recognise and fulfil their God given gifts and abilities. Through a creative, inclusive curriculum, we inspire all to be lifelong learners, equipped with the skills needed to be thankful, generous members of society.

Our Bible Narratives:

The Bible narratives referencing God/Jesus as: 'The Good Shepherd,' come from both the New and Old Testament.

Explaining our Bible references

Our Vision at Hartlip School is embedded in the imagery of God/Jesus as the Good Shepherd. We draw upon these images in both the Old and the New Testament of the Bible. We believe that our daily living in school, directed by our values draws parallels to that of a shepherd taking care of his sheep.

Our Christian School Values are: Friendship, Forgiveness, Peace, Trust and Thankfulness

Friendship: As the Good Shepherd cares for every member of the flock, we live together in friendship. In learning to live, we accept that not every person may be our friend and at times, we may, like the Lost Sheep, lose our way. Despite our difficulties, we are all still members of the same flock. We care for each other and treat others in the way we would like to be treated ourselves.

Forgiveness: In order to live in friendship, we must learn forgiveness. We recognise that in living together, we will make mistakes. We understand that to live in friendship with each other, we must learn to forgive each other, in the same way that God forgives us:

"forgive each other, just as in Christ God forgave you."

We teach that we learn from our mistakes. By forgiving others, we ensure that we live in friendship:

"Be kind and compassionate to one another, **forgiving** each other, just as in Christ God forgave you."

Peace: When living in friendship with each other and learning to forgive each other, we experience



peace. This learning extends beyond our school community in to society. To live in a peaceful world, we need to cascade friendship and forgiveness.

Trust: As the sheep trust the shepherd to take care of them, we learn that Christians believe God takes care of us. Our school community is a safe environment where all can flourish. Children and parents trust staff to provide a nurturing, caring and safe environment where all can fulfil their God given gifts and abilities. Children, parents and staff trust the leadership of the school to ensure their safety in an environment whereby everyone can thrive. In the same way that a shepherd protects sheep from all harm and danger, the school does likewise for its members.

Thankfulness: Just as a sheep is thankful for the safety of a rich environment, so too are we thankful for our school community and all that it offers. We learn to be outward looking, thinking about 'we', as opposed to 'me'. We try in all things to 'give thanks,' to be grateful for what we have and to give to others less fortunate than ourselves. We seek to serve and extend this learning in to a wider world, learning to live!

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary consequences for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of *the school*, but is linked to membership of the school/academy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities:

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about online safety incidents and monitoring reports. Mrs Jane Davies is the Online Safety Governor as [Safeguarding Governor](#).

The role of the Online Safety *Governor* includes:

- regular meetings with the Online Safety Co-ordinator/officer
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors/Board/Committee/meeting



Headteacher and Senior Leaders

- The *Headteacher* has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents– “Responding to incidents of misuse” and relevant *Local Authority* disciplinary procedures).
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Online Safety Lead: Headteacher

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Safeguarding *Governor* to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of Governors
- reports regularly to Senior Leadership Team

Network Manager/Technical staff

Those with technical responsibilities are responsible for ensuring:

- that the school’s technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- 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 online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school/academy online safety policy and practices
- they have read, understood and signed the staff acceptable use policy.
- they report any suspected misuse or problem to the Headteacher 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
- online safety issues are embedded in all aspects of the curriculum and other activities
- students/pupils understand and follow the Online Safety Policy and acceptable use policies
- students/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, 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 students/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/Designated Person/Officer

Should be trained in online 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
- online-bullying

Students/Pupils:

- are responsible for using the *school* digital technology systems in accordance with the student/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 online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school's/academy's* online safety policy covers their actions out of school, if related to their membership of the school

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature.

Parents and carers will be encouraged to support the school in promoting good online 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/Learning Platform and on-line student/pupil records
- their children's personal devices in the school/academy (where this is allowed)

Community Users

Community Users who access school systems or programmes as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school/academy systems.

Education – Students/Pupils

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

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:

- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Pupils are 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 are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are 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.



- Students/pupils are helped to understand the need for the student/pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school/academy.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, pupils will 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 are 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, 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 online 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 online 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 school will seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, Learning Platform
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications
- Education – The Wider Community

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school/academy website will provide online safety information for the wider community
- Sharing their online safety expertise/good practice with other local schools
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision



Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows: [\(select/delete as appropriate\)](#)

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school/academy online safety policy and acceptable use agreements.
- The Headteacher (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Headteacher (or other nominated person) will provide advice/guidance/training to individuals as required

Training – Governors

Governors will take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/MAT/National Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in school/ training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Technical – infrastructure/equipment, filtering and monitoring

The school is 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

- 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 technical systems
- Servers, wireless systems and cabling will be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by Carl Adams
- The “master/administrator” passwords for the school systems, used by the Network Manager must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place.
- Carl Adams is 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 by actively employing the Internet Watch Foundation CAIC list.
- Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- users report any actual/potential technical incident/security breach to the Headteacher
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- 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 (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school’s wireless network. The device then has access to the wider internet which may include the school’s learning platform and other cloud-based services such as email and data storage. All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s online safety education programme.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:



- When using digital images, staff will inform and educate students/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 students/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 school/academy 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 pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school/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 school/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 pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

The school will ensure that:

- it has a Data Protection Policy.
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. The school/academy may also wish to appoint a Data Manager and Systems Controllers to support the DPO



- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy' to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- it provides staff, parents and volunteers, teenagers with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- procedures are in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it [reports any relevant breaches to the Information Commissioner](#) within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- It has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter.
- Staff undertaking particular data protection functions, such as handling requests under the



- individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data is encrypted and password protected.
- device is password protected.
- device is protected by up to date virus and malware checking software
- data is securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any school/academy personal data to personal devices except as in line with school policy
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

Communications

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

- The official school email service is regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students/pupils should therefore use only the school/academy email service to communicate with others when in school, or on school/academy systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school 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 parents/carers must be professional in tone and content.
- Whole class/group email addresses may be used at KS1, while students/pupils at KS2 and above will be provided with individual school email addresses for educational use.



- Pupils will be taught about online safety issues, such as the risks attached to the sharing of personal details. They are 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

Hartlip School understands that it and local authorities have a duty of care to provide a safe learning environment for pupils and staff. It could be held responsible, indirectly for acts of employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority to the injured party. Reasonable steps to prevent predictable harm are in place.

The school 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 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 *school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school/ academy, it must be made clear that the member of staff is not communicating on behalf of the school/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 school 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 pro-actively monitor the Internet for public postings about the school
- The school will effectively respond to social media comments made by others according to a defined policy or process

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. 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 a school/ context, either because of the age of the users or the nature of those activities.

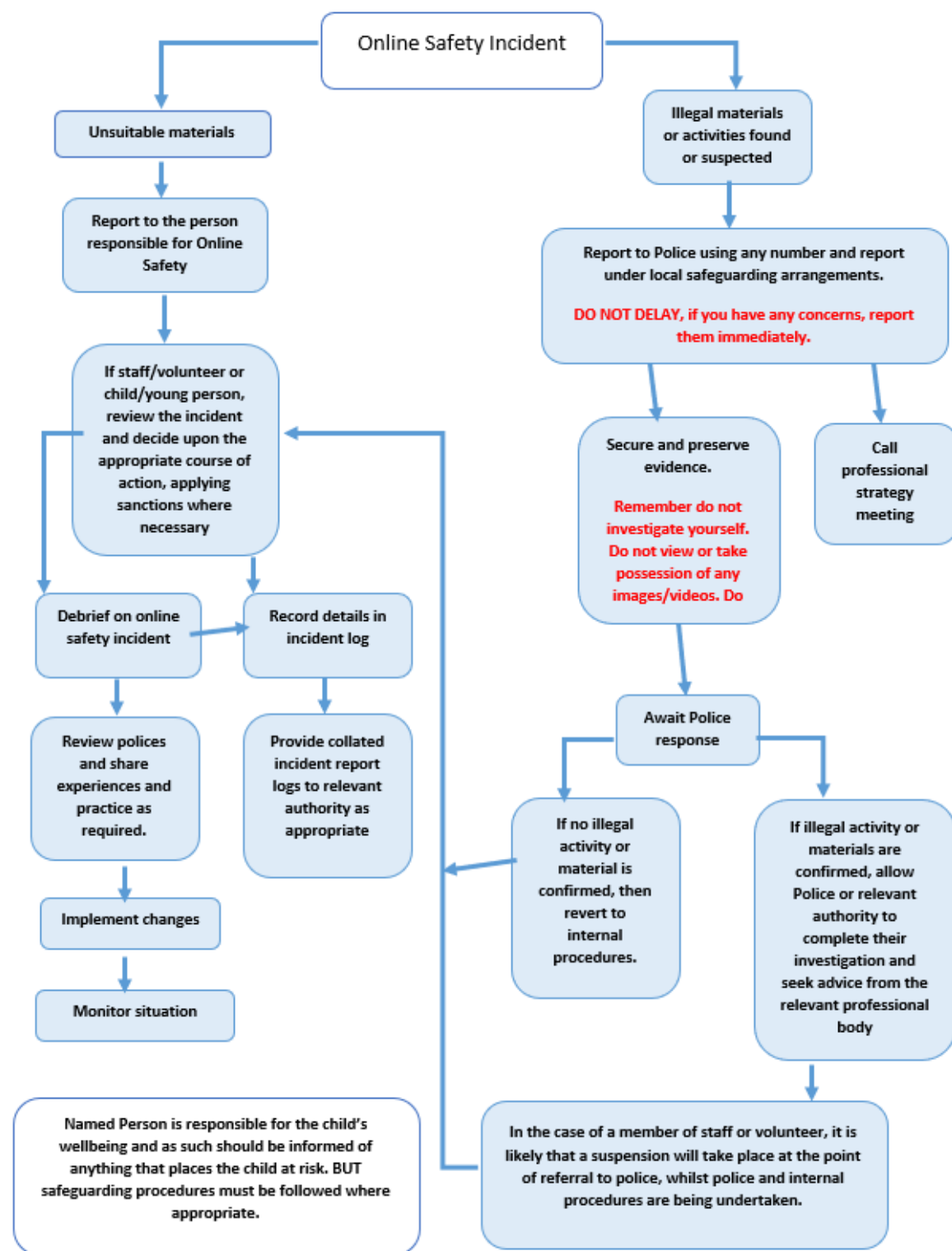
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems.

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

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.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school/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 will 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/Academy Group or national/local organisation (as relevant).
 - Police involvement and/or action

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

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- offences under the Computer Misuse Act (see User Actions chart above)
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the *school/academy* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes.



School actions & sanctions

It is more likely that the school/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 school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.