Gillotts School

E-Safety Policy

Introduction

This policy which will consider all current and relevant issues linked to e-safety, in a whole school context, linking with other relevant policies, such as the Child Protection (including Prevent), Behaviour for Learning and Anti-Bullying policies. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Schools must, through their e-safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. We also have a responsibility to ensure that children are safe from terrorist and extremist material when accessing the internet in schools.

This policy was approved by Governors on 23 February 2016. The implementation of this policy will be monitored by the Deputy Headteacher (Curriculum) and the IT Services Manager, who is the e-safety coordinator. The policy will be reviewed annually.

Scope of the Policy

This policy applies to all members of the school community (including staff, students, parents, volunteers, visitors) who have access to and are users of school ICT 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 when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour for Learning policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

Governors
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The link Governor for Child Protection also acts as e-safety governor.

Headteacher
The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the e-safety coordinator. The Headteacher is responsible for ensuring that the e-safety coordinator receives suitable training to enable him/her to carry out the e-safety roles and to train other colleagues, as relevant.

E-Safety Coordinator:
The IT Services Manager acts as the e-safety coordinator, supported by the Headteacher who is the designated person for Child Protection.
The e-safety coordinator:
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and procedures
- 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 the LADO
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, meets regularly with the Headteacher to discuss current issues, review incident logs and filtering/ change control logs
- reports regularly to Leadership Team

IT Services Manager:
The IT Services Manager is 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 e-safety technical requirements
- that users access the network and, where possible, 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 e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that monitoring software/ systems are implemented and updated as agreed, in order that any misuse/attempted misuse can be reported to the Headteacher

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 school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headteacher or e-safety coordinator for investigation
- all digital communications with students and parents should be on a professional level and only carried out using official school systems; all communication with students should be to their school email address
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the e-safety and acceptable use policies
- 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 school activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, it is best practice for students to 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 Person for Child Protection
The Designated Person for Child Protection should be trained in e-safety issues and be aware of the potential for serious 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

E-Safety Group
The functions of the e-safety Group are delivered by the group that undertakes strategic planning for IT within the school which is led by the Deputy Headteacher (Curriculum).

This group assists the e-safety coordinator with:

- the production/ review/ monitoring of the school e-safety policy and procedures
- the production/ review/ monitoring of the school filtering policy (and requests for filtering changes)
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network/ internet/ incident logs
- consulting stakeholders, including parents and students, about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool

Students
Students are responsible for:

- using the school digital technology systems in accordance with the Student Acceptable Use Policy
- having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- understanding the importance of reporting abuse, misuse or access to inappropriate materials and knowing how to do so
- knowing and understanding 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
- understanding the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school.

Parents
Parents 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 and information about national/ local e-safety campaigns/ literature. Parents and carers will be encouraged to support the school in promoting good e-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 records
- their children's personal devices in the school.

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 the 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.

E-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 will be provided as part of the PSHE curriculum
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial activities
- Students will 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students 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
- Students will be helped to understand the need for the student Acceptable Use Policy 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 will 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that IT Services can temporarily remove those sites from the filtered list for the period of study. Any request to do so will be auditable, with clear reasons for the need.

Education – parents

Many parents have only a limited understanding of e-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 school will therefore seek to provide information and awareness to parents and carers through:

- Information evenings
- Letters, newsletters, website
- High profile events/ campaigns eg Safer Internet Day

Education & Training – Staff

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

- A planned programme of formal e-safety training will be made available to staff, as part of their training in Child Protection. This will be regularly updated and reinforced.
  Note SWGfL BOOST includes unlimited online webinar training for all, or nominated, staff (http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Professional-Development)
- All new staff should receive e-safety training as part of their induction programme, linked to their Child Protection training, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- The e-Safety coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

- The e-safety coordinator will provide advice/ guidance/ training to individuals as required.

Training – Governors

Governors should take part in e-safety awareness sessions, with particular importance for those who are members of the Curriculum and Student Progress Committee. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation (eg SWGfL)
- Participation in school training sessions, eg for staff or parents

Technical – infrastructure/ equipment, filtering and monitoring

The 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 ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- 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 must 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 the IT Services Manager 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 staff will be required to change their password regularly
- The "master/ administrator" passwords for the school ICT system, used by the IT Services Manager must also be available to the Headteacher and kept in the school safe
- The IT Services Manager 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 actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and can be monitored if there is a concern. 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
- The school has provided enhanced/ differentiated user-level filtering
- School technical staff are able to monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy
- Users report any actual/ potential technical incident/ security breach to IT Services via the IT Services help desk
- 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. The school infrastructure and individual workstations are protected by up to date virus software
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems
- An agreed policy is in place regarding the extent of personal use that 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 download executable files and install programs on i-pads but does not allow this on other school devices
- An agreed policy is in place (see Staff Handbook) regarding the use of removable media (eg 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.

Bring Your Own Device (BYOD)

- The school has a set of clear expectations and responsibilities for all users set out in the BYOD policy and procedures
- The school adheres to GDPR (2018)
- All users are provided with and accept the Acceptable Use Policy
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken by all staff
- Students receive training and guidance on the use of personal devices
- Monitoring of usage in the classroom will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

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 and students 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 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 eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents are welcome 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 comment on any activities involving other students 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. These images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/ video images that 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 in association with photographs.
- We will obtain written consent from parents/carers for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

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 to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. Details of the DPO are included in the Data Protection Policy.
- 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 the minimum personal data necessary to enable it to perform its function and, where possible, it will not hold it for longer than necessary for the purposes it was collected for. The school has 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 and the school has systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- It provides staff, parents, volunteers, and students 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 (DIPA) 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 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 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 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
- Consideration has been given to the protection of personal data when accessed using any remote access solutions
- There is a Freedom of Information policy which sets out how the school 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

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 understands their rights and know how to handle a request whether verbal or written, and 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 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

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

- the data must be encrypted and 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

See Staff Handbook for more details.

Communications

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

When using communication technologies the school considers the following as good practice:
- The official school email service may be regarded as safe and secure and data may be recovered using the back-up system. Users should be aware that email communications are accessible by the Headteacher in connection with a concern or an investigation. Staff and students should therefore use only the school email service to communicate with others.
- Users must immediately report, to the IT Services Manager, 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 staff and parents must be professional in tone and content. These communications may only take place using official (monitored) school systems. Staff personal email addresses, text messaging or social media must not be used for these communications.
- Students will be taught about e-safety issues, such as the risks attached to the sharing of personal details. They will 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.

Social Media - Protecting Professional Identity

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through:
- Ensuring personal information is not published
- 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

School staff should ensure that:
- No reference should be made in personal social media accounts to students, parents or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Personal Use:
- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school/academy or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school/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 pro-actively 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 school's use of social media for professional purposes will be checked regularly by the e-safety coordinator to ensure compliance with the e-safety policy.

See 'Guidance for safer working practice' for more details.

Unsuitable/ inappropriate 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 school or outside school when using school equipment or systems. The school policy restricts usage as follows:

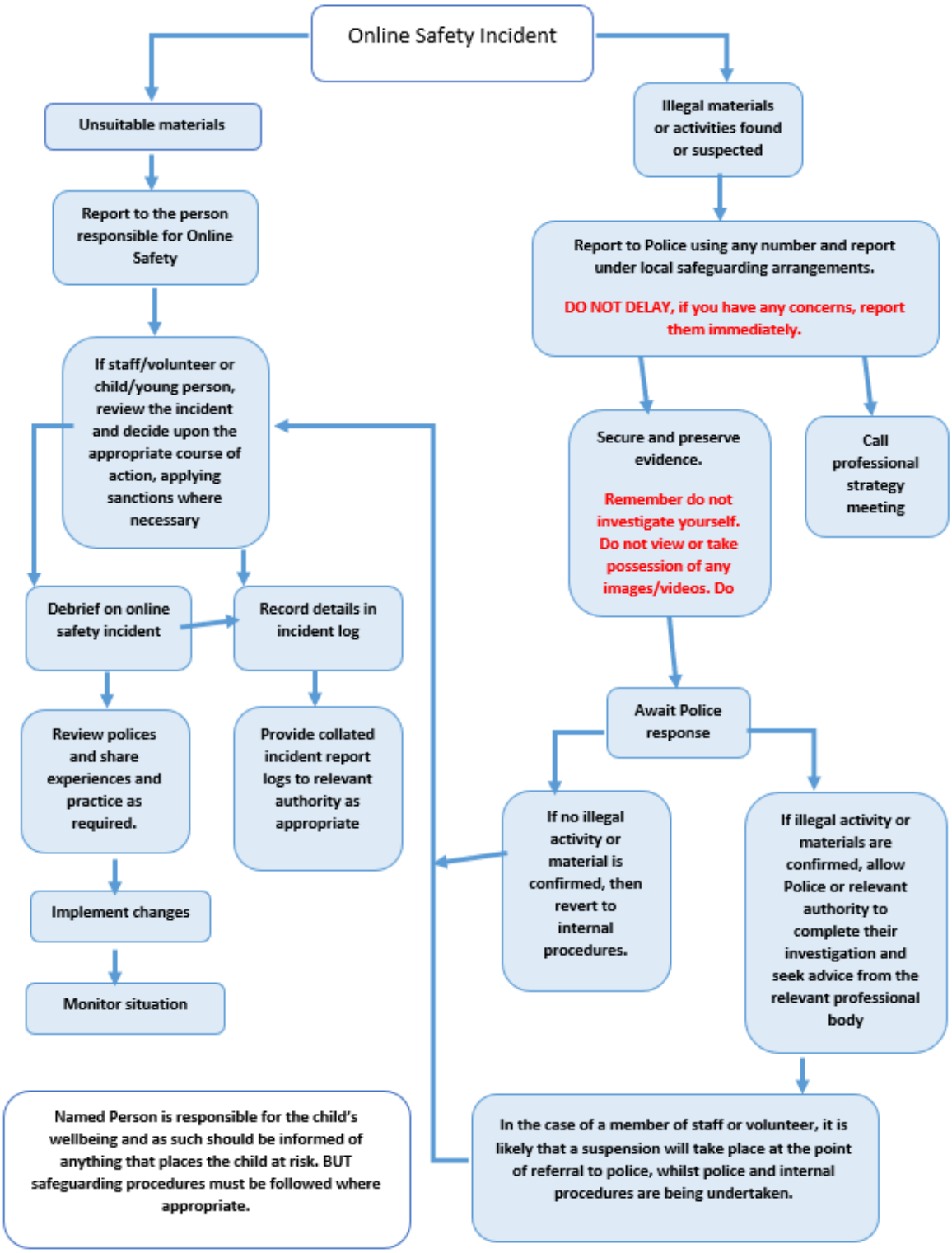
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children. Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character). Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files						X

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
• Revealing or publicising confidential or proprietary information (eg. financial/ personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment without relevant permission)					
Infringing copyright					X
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer/ network access codes and passwords)				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gambling		X			
On-line gaming (non-educational)		X			
On-line gaming (educational)		X			
On-line shopping / commerce		X			
File sharing		X			
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting eg Youtube		X			

Responding to incidents of misuse

Illegal Incidents

If there is any suspicion that the website(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) for responding to online safety incidents and report immediately to the police.



<u>Other Incidents</u>

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible use 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 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 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.

School Actions & Sanctions

It is more likely that the school 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.

Incidents of misuse by students will be dealt with in accordance with the Behaviour for Learning Policy. If students deliberately access or try to access material that could be considered illegal, the matter will be referred to the police. As a consequence for serious misuse of the school's IT systems, access to the systems may be restricted/ withdrawn.

Incidents of misuse by staff will be dealt with in accordance with the Disciplinary Procedure. If staff deliberately access or try to access material that could be considered illegal, the matter will be referred to the police.