Brant Broughton CE Methodist Primary School

Online Safety Policy

April 2020

SWGfL
Safe, Secure, Online

Development/Monitoring/Review of this Policy

This online safety policy has been developed by the Headteacher, all teaching staff and ICT support staff. Staff training on e-safety takes place annually for all staff as part of our Safeguarding Training. It will be reviewed every two years.

The school will monitor the impact of the policy using: (delete/add as relevant)

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Surveys/questionnaires of
    - o   students/pupils
    - o   parents/carers
    - o   staff

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/academy digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the schoolsite and empowers members of staff to impose disciplinary penalties 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. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 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. A member of the Governing Body (Chris Fisher) has taken on the role of Online Safety Governor. The role of the Online Safety Governor/Director will include:

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

Headteacher

- has a duty of care for ensuring the safety (including online safety) of members of the school community and the day to day responsibility for online safety.
- and Senior Teacher (Mrs Simeoli) are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff as outlined on the Safeguarding posters in the staff room and main office with LADO contact.
- is 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.
- 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/relevant body
- 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 Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of Governors

Technical staff (F1)

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 and Senior Leaders; for investigation/action/sanction
- 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 online safety policy and practices**
- **they have read, understood and signed the staff acceptable use agreement**
- **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

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/academy 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 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

Policy Statements

Education – Students/Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of spupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. 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 should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- **A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited**
- **Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities for example, during Internet Safety Day in February each year.**
- **Students/pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.**
- **Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- **Students/pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.**
- **Pupils should be helped to understand the need for the student/pupil 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 pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.**

- **Where students/pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.**
- **It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) 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/academy will therefore seek to provide information and awareness to parents and carers through:

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

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:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should 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.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead will receive regular updates through attendance at external training events (e.g. Safeguarding Briefings) 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 Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Governors should 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 Governors Briefings/or other relevant organisation (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents and as part of governor visits to school

The school will be responsible for ensuring that the school/academy 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 online 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**
- **All users will have clearly defined access rights to school technical systems and devices.**
- **The Headteacher 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.**
- **The school has provided enhanced/differentiated user-level filtering, allowing different filtering levels for different groups of users – staff/pupils etc)**
- **Users to report any actual/potential technical incident/security breach to the Headteacher.**
- **The school infrastructure and individual devices are protected by up to date virus software.**

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. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

- **The school acceptable use agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies**
- **The school allows:** (the school should complete the table below to indicate which devices are allowed and define their access to school systems)

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes	Yes	No[2]	Yes	Yes

---

[2] The school should add below any specific requirements about the use of mobile/personal devices in school. The Acceptable Use document signed by staff and visitors specifies that personal devices can only be used in the staffroom and office areas.

Full network access	Yes	Yes	Yes			

Aspects that the school may wish to consider and be included in their online safety policy, mobile technologies policy or acceptable use agreements:

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for 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/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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school/academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school 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.

Data Protection

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

The school must 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.**

- **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, volunteers with information about how the school/academy looks after their data and what their rights are in a clear Privacy Notice** (displayed on the school website)
- **procedures must be 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 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.**
- **If a maintained school/academy, it must have 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 must be encrypted and password protected.**
- **device must be password protected.**
- **device must be protected by up to date virus and malware checking software**
- **data must be securely deleted from the device, in line with school/academy 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 understands 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 may be 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 email service to communicate with others when in school, or on school systems (e.g. by remote access).
- **Users must immediately report, to the nominated person – in accordance with the school/academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- **Any digital communication between staff and students/pupils or parents/carers (email, social media, chat, blogs, etc) must be professional in tone and content.** These communications may only take place on official (monitored) schoo systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students/pupils should be taught about online 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.

Social Media - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their 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 liable to the injured party.   Reasonable steps to prevent predictable harm must be 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 communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

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

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/academy when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload,	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X

data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	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 • Revealing or publicising confidential or proprietary information (e.g. 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)						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 (e.g. 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	
Using school systems to run a private business					X	
Infringing copyright					X	
On-line gaming (educational)					X	
On-line gaming (non-educational)					X	

On-line gambling				X	
On-line shopping/commerce			X		
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube			X		

Responding to incidents of misuse

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

Illegal Incidents

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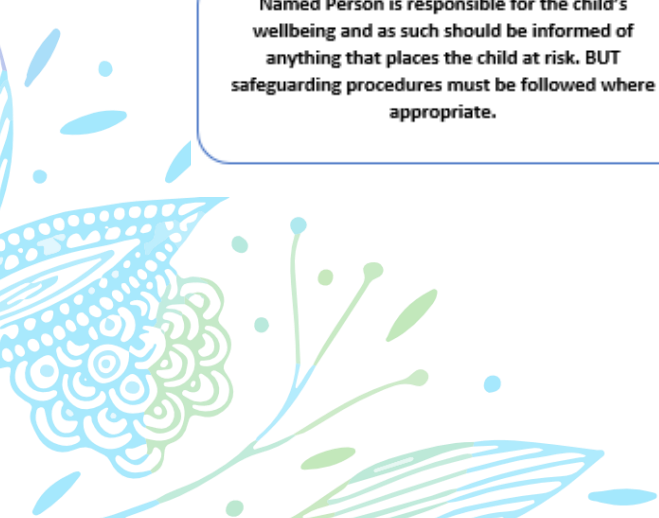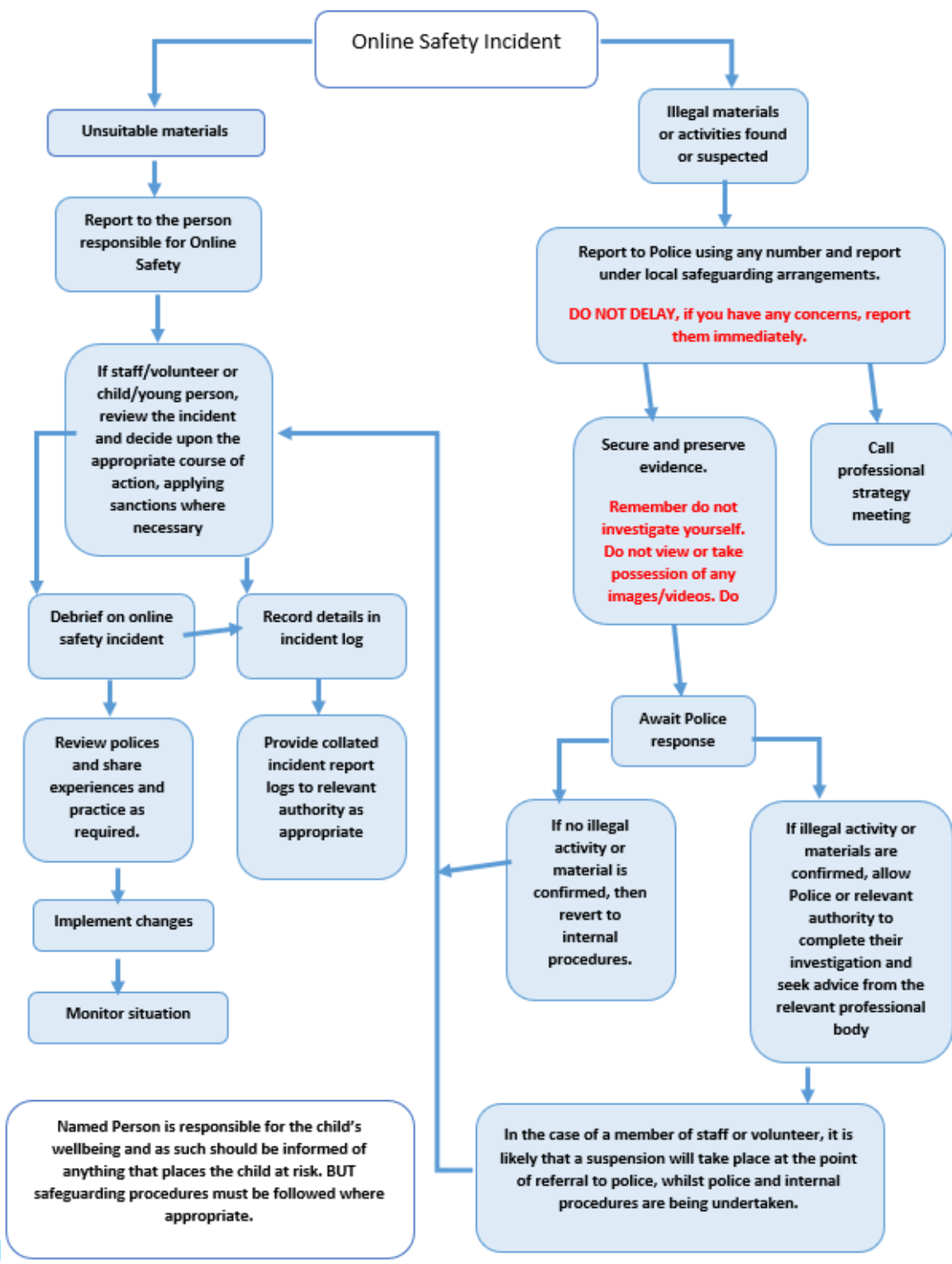
Other Incidents

It is hoped that all members of the school/academy 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 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/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 and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

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. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures to be discussed according to the nature and seriousness of the incident and also the pupil or member of staff concerned. In the case of pupil sanctions, parents are informed as soon as possible including where incidents occur outside of school. All incidents and actions/sanctions are recorded using the template in the Appendices section.

Student/Pupil Acceptable Use Agreement Template – KS2

School policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These 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. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the students/pupils to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep any usernames and passwords safe and secure – I will not share it, 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 be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- 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 use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.
- I will act as I expect others to act toward me:
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, 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 not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed
- When using the internet for research or recreation, I recognise that:
- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student/Pupil Acceptable Use Agreement Form

This form relates to the pupil acceptable use agreement; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

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

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.

Name of Pupil: ....

Class: ....

Signed: ....

Date: ....
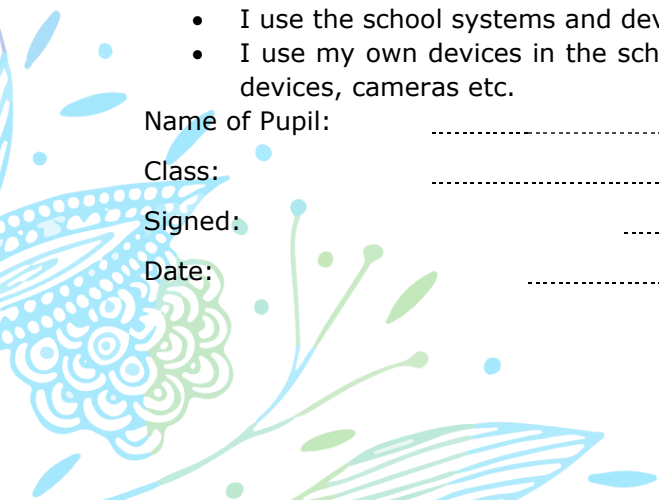
Student/Pupil Acceptable Use Policy Agreement Template – (Foundation/KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child): ....

Responding to incidents of misuse – flow chart

```
                        Online Safety Incident
           ┌────────────────────┴──────────────────────┐
           ▼                                            ▼
  ┌──────────────────┐                        ┌──────────────────┐
  │ Unsuitable       │                        │ Illegal materials│
  │ materials        │                        │ or activities    │
  └──────────────────┘                        │ found or         │
           │                                   │ suspected        │
           ▼                                   └──────────────────┘
  ┌──────────────────┐                                  │
  │ Report to the    │                                  ▼
  │ person           │                        ┌──────────────────────┐
  │ responsible for  │                        │ Report to Police      │
  │ Online Safety    │                        │ using any number and  │
  └──────────────────┘                        │ report under local    │
           │                                   │ safeguarding          │
           ▼                                   │ arrangements.         │
  ┌──────────────────┐                        │ DO NOT DELAY, if you  │
  │ If staff/        │◄───────────┐           │ have any concerns,    │
  │ volunteer or     │            │           │ report them           │
  │ child/young      │            │           │ immediately.          │
  │ person, review   │            │           └──────────────────────┘
  │ the incident and │            │              ┌───────┴────────┐
  │ decide upon the  │            │              ▼                ▼
  │ appropriate      │            │      ┌──────────────┐  ┌────────────┐
  │ course of action,│            │      │ Secure and    │  │ Call        │
  │ applying         │            │      │ preserve      │  │ professional│
  │ sanctions where  │            │      │ evidence.     │  │ strategy    │
  │ necessary        │            │      │ Remember do   │  │ meeting     │
  └──────────────────┘            │      │ not           │  └────────────┘
     │            │               │      │ investigate   │
     ▼            ▼               │      │ yourself.     │
┌──────────┐ ┌──────────┐         │      │ Do not view   │
│ Debrief  │→│ Record   │         │      │ or take       │
│ on online│ │ details  │         │      │ possession of │
│ safety   │ │ in       │         │      │ any images/   │
│ incident │ │ incident │         │      │ videos. Do    │
└──────────┘ │ log      │         │      └──────────────┘
     │       └──────────┘         │              │
     ▼            │               │              ▼
┌──────────┐      ▼               │      ┌──────────────┐
│ Review   │ ┌──────────┐         │      │ Await Police │
│ polices  │ │ Provide  │         │      │ response     │
│ and share│ │ collated │         │      └──────────────┘
│ experien-│ │ incident │         │        ┌────┴────┐
│ ces and  │ │ report   │         │        ▼         ▼
│ practice │ │ logs to  │   ┌─────────────────┐ ┌──────────────┐
│ as       │ │ relevant │   │ If no illegal   │ │ If illegal   │
│ required.│ │ authority│   │ activity or     │ │ activity or  │
└──────────┘ │ as       │   │ material is     │ │ materials are│
     │       │ appropri-│   │ confirmed, then │ │ confirmed,   │
     ▼       │ ate      │   │ revert to       │ │ allow Police │
┌──────────┐ └──────────┘   │ internal        │ │ or relevant  │
│ Implement│                │ procedures.     │ │ authority to │
│ changes  │                └─────────────────┘ │ complete     │
└──────────┘                                      │ their        │
     │                                            │ investigation│
     ▼                                            │ and seek     │
┌──────────┐                                      │ advice from  │
│ Monitor  │                                      │ the relevant │
│ situation│                                      │ professional │
└──────────┘                                      │ body         │
                                                  └──────────────┘
```

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Reporting Log

Group: ....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Training Needs Audit Log

Group: ....

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date