Online Safety Policy 2023-25

This policy was updated: April 2023

This policy will be reviewed: January 2025

Signed by Headteacher: ……

Signed by Chair of Governors: ……

Date: ……

1. Scope of the policy 4
2. Aims of this policy: 4
3. Policy development, monitoring and review 4
4. Acceptable use agreements 5
5. Roles and responsibilities 5
a. Headteacher and senior leaders 6
b. School Governors 6
c. Online Safety Lead (OSL) 6
d. Designated Safeguarding Lead (DSL) 7
e. Curriculum leads 7
f. Teaching staff, support staff and volunteers 7
g. Network manager & technical staff 8
h. Pupils 8
i. Parents 9
6. Reporting and Responding 9
7. Education and training 10
a. Education of pupils 10
b. Contribution of pupils 11
c. Staff and volunteers 11
d. Governors 12
e. Parents 12
8. Technology 13
a. Filtering 13
b. Monitoring 14
c. Technical security 14
d. Mobile technologies (including BYOD/BYOT) 15
e. Digital and video images: 16
f. Online publishing 17
g. Data protection 17
10. Social media 17
a. School use: 17
b. Personal use 18
c. Monitoring of social media 18
d. Cyberbullying (including 'sexting') 19
11. Outcomes 19
12. Handling of complaints 20
13. Relevant policies 20
APPENDICES 21
ONLINE SAFETY POLICY APPENDIX 1 - Staff and Volunteer Acceptable Use Agreement 22
ONLINE SAFETY POLICY APPENDIX 2 - Pupil Acceptable Use Agreement (EYFS and KS1) 23
ONLINE SAFETY POLICY APPENDIX 3 - Pupil Acceptable Use Agreement (KS2) 24
ONLINE SAFETY POLICY APPENDIX 4 - Online Safety Incident Flowchart 26
ONLINE SAFETY POLICY APPENDIX 5 - Procedures to handle incidents of misuse, including responding to illegal incidences 27

1. Scope of the policy

- This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents and visitors) who have access to and are users of school's digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site where allowed.
- The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils 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 cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the school but are linked to membership of the school.
- The 2011 Education Act and The Schools (Specification and Disposal of Articles) Regulations 2012 increased these powers with regard to the searching for and of electronic devices and the deletion of data as well as the guidance from the DfE entitled Screening, Searching and Confiscation at schools (DfE 09/22)
- The school will deal with such incidents within this policy and associated policies as referenced above and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

2. Aims of this policy:

The Online School Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements and flowcharts
- is made available to staff at induction and through normal communication channels
- is published on the school website.

3. Policy development, monitoring and review

This Policy has been developed by a working group made up of:

- Headteacher and senior leaders
- Online Safety Lead
- Staff – including teachers, support staff and technical staff

- Governors

The school will monitor the impact of the policy using:

- logs of reported incidents
- monitoring logs of internet activity (including sites visited)/filtering
- internal monitoring data for network activity
- surveys/questionnaires of
  - pupils
  - parents
  - staff

4. Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the schools. The acceptable use agreements will be communicated and reinforced through:

- all areas of the school's curriculum and school assemblies
- communication with parents
- staff induction and the staff code of conduct/handbook
- the school website

5. Roles and responsibilities

- To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learn from each other and from good practice elsewhere, report inappropriate online behaviours, concerns, and misuse as soon as these become apparent. Whilst this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.
- Staff should always maintain appropriate professional boundaries, avoid behaviour which could be misinterpreted by others and report any such incident to a senior manager. This is as relevant in the online world as it is in the classroom; staff engaging with pupils and/or parents online have a responsibility to model safe practices at all times.
- In addition to the roles and responsibilities outlined below, and to support the implementation of this policy, the school has compiled 'Acceptable Use Agreements' (AUAs), which provide clear guidance in relevant areas such as conduct, access to and use of the school system, removable media, downloading files, sharing information, social networks and devices (both school and personal equipment within and outside school).
- Separate agreements have been written for:
  - EYFS and key stage one pupils
  - key stage two pupils
  - staff and governors (additionally in Staff Code of Conduct)
  - volunteers (Good Practice Guide for Volunteers and External Agency representatives working in school)

who are all expected to read and sign them to acknowledge their responsibilities in this area.

a. Headteacher and senior leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members' of the school community and fostering a culture of safeguarding, though the day to day responsibility for online safety will be delegated to the Online Safety Lead (OSL).
- The Headteacher and (at least) another member of the senior management team (SMT) 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. (Appendix 5 – 'Procedures to handle incidents of misuse, including responding to illegal incidences (flow chart)' and relevant Local Authority disciplinary procedures).
- The Headteacher and SMT are responsible for ensuring that the OSL 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 SMT 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.
- The Headteacher and SMT will receive monitoring reports from the OSL.

b. School Governors

- A member of the Governing Body has taken on the role of the Online Safety Governor and the governor with that responsibility is Stephen Uncles.
- Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.
- The role of the Online Safety Governor will include:
    - meetings with the OSL
    - receiving (collated and anonymised) reports of online safety incidents
    - checking that provision outlined in this Online Safety Policy (e.g. online safety education provision and staff training) is taking place as intended
    - reporting to relevant Governors/Committee/meeting

c. Online Safety Lead (OSL)

The OSL will be a member of the SMT and their responsibilities are to:

- work closely on a day to day basis with the DSL
- take day to day responsibility for online safety, being aware of the potential for serious child protection concerns
- have a leading role in reviewing the school's online safety policy, procedures and documents
- promote an awareness and commitment to online safety education/awareness, raising concerns across the school and beyond
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place (i.e. misuse – see Appendix 5)

- provide (or identify sources of) training and advice for staff, governors, parents and pupils
- be aware of external sources of support and guidance in dealing with online safety issues (e.g. local authority, police etc) and liaise with the Local Authority (LA) and other external agencies as relevant
- liaise with the school's technical support and external providers
- receive and log online safety incidents to inform practice, policy review and development
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and, if possible filtering and monitoring logs
- attend relevant meetings
- report regularly to the STM
- review emerging technologies for educational benefit and a carry out a risk assessment before use in school is allowed.

d. Designated Safeguarding Lead (DSL)

The DSL should be trained in online safety and be aware of the potential for serious child protection and safeguarding issues to arise from:

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

e. Curriculum leads

- Curriculum Leads will work with the OSL to develop a planned and coordinated online safety programme (e.g. ProjectEVOLVE), with reference to the DfE guidance: 'Teaching online safety in schools' (January 2023).
- This will be provided through:
    - a discrete programme
    - PHSE and RHE/SRHE programmes
    - a mapped cross-curricular programme
    - assemblies and pastoral programmes
    - through relevant initiatives and opportunities (e.g. Safer Internet Day and Anti-Bullying Week

f. Teaching staff, support staff and volunteers

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable AUA
- they immediately report any suspected misuse or problem to the DSL/DDSL for investigation/action, in line with the school safeguarding procedures

- all digital communications with learners and parents should be on a professional level, professional in tone and content and only carried out using official school systems, emails and technologies that are officially sanctioned by the school
- online safety issues are embedded in all aspects of the curriculum and other activities
- learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use
- processes are in place for dealing with any unsuitable material that is found in internet searches
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource
- they have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

g. Network manager & technical staff

The network manager/technical staff is responsible for ensuring that:

- they are aware of and follow the school's Online Safety Policy and Technical Security Proceudres to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the local authority/MAT or other relevant body
- there is clear, safe and managed control of user access to networks and devices
- 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
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to DSL/DDSL for investigation and action
- the filtering procedures are applied and updated on a regular basis and their implementation is not the sole responsibility of any single person
- monitoring software/systems are implemented and regularly updated as agreed in school policies

h. Pupils

Pupils are responsible for using the school's digital technology systems in accordance with the learner AUA and Online Safety Policy.

- They should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- They should know what to do if they, or someone they know, feels vulnerable when using online technology.
- Pupils should understand the importance of adopting good online safety practices 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.

i. Parents

- Parents play a crucial role in ensuring that their children understand the need to use internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through:
    - publishing the school Online Safety Policy on the website
    - parents' evenings
    - newsletters and letters
    - the school's website and learning platform
    - information about national and local online safety campaigns
- Parents will be encouraged to support the school in:
    - reinforcing the online safety messages provided to pupils in school
    - following guidance on the appropriate use of digital and video images taken at school events and in their access to parents sections on the school's website, learning platforms and online pupil records
    - following the school's guidance on the use of their children's personal devices in the school (where this is allowed)

6. Reporting and Responding

- It is more than 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 the members of the school community are aware that incidents have been dealt with. Such incidents of misuse will be dealt with through the school's normal behaviour and disciplinary procedures.
- There may however be occasions when the school has to respond to reports of illegal misuse and, whilst the school will take all reasonable precautions to ensure online safety for all school users, we recognise that incidents may occur inside and outside of the school (with impact on the school) which will need intervention.
- All staff will be made aware of the Appendices 4 and 5: "Online Safety Incident" (Appendix 4) and "Responding to Incidents of misuse" (Appendix 5).
- It is important that those reporting an online safety incident have confidence that the report will be treated seriously, and dealt with effectively and that there are support strategies in place (e.g. peer support) for those reporting or affected by an online safety incident.
- The school will ensure that:
    - there are clear reporting routes which are understood and followed by all members of the school community, which are consistent with the school's

safeguarding procedures (including the management of allegations) as well as the school's policies on whistleblowing and complaints
    - all members of the school community are aware of the need to report online safety issues/incidents
    - reports will be dealt with as soon as is practically possible, once they are received
    - those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions as relevant
- the DSL and OSL, together with other responsible staff, will have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm, (see flowchart and user actions chart in Appendix 5) the incident must be escalated through the agreed school safeguarding procedures.
- Incidents should be logged using the school's system.

7. Education and training

a. Education of pupils

- Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety and digital literacy is therefore an essential part of the school's online safety provision and should be effectively threaded through the appropriate pillars in other curriculum areas.
- Pupils should be helped to understand the need for the 'Pupil Acceptable Use Agreement' and encouraged to adopt safe and responsible use both within and outside school.
- The school curriculum is designed and written with reference to the key documents listed below, ensuring breadth and progression in the content to reflect the different and escalating risks that pupils face and covering the principles of online safety:
    - Teaching online safety in schools (DfE Published June 2019/updated January 2023)
    - Education for a Connected World framework (2020 Edition published by the UK Council for Internet Safety)
    - SWGfL Project Evolve – online safety curriculum programme and resources
    - Computing Curriculum (DfE 2013)
- To ensure the quality of learning and outcomes, the online safety curriculum should be broad, up-to-date, provide opportunities for creative activities and context-relevant with agreed objectives, leading to clear and evidenced outcomes.
- Given the rapid changes in this area the school's provision should be regularly revisited.
- Pupils need the help and support of the school to recognise and avoid online safety risks and build their resilience. This includes:
    - how to use technology safely, responsibly, respectfully and securely
    - where to go for help and support when the have concerns about content or contact on the internet or other online technologies.

- The programme will be accessible to learners of different ages and abilities such as those with additional learning needs or those with English as an additional language.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of the information.
- As part of the relationship and health education curriculum, pupils are taught about online safety and harms. This includes being taught:
  - what positive, healthy and respectful online relationships look like
  - the effects of online actions on others
  - how to recognise and display respectful behaviours on line
- Key on line safety messages should also be reinforced as part of a planned programme of assemblies and pastoral activities.
- 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.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites they visit
  - It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would require them to access sites normally blocked by the school's filtering system. In such cases, staff can request that filters can be temporarily removed from those sites for the period of study. Any request to do so, should be auditable, with clear reasons for the need and in line with the school's procedures.
  - Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

b. Contribution of pupils

- The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised:
  - through mechanisms to canvass pupil feedback and opinions
  - by pupil representation through the digital leaders
  - through pupils representation on the online safety education programme, e.g. peer education, digital leaders, leading lessons for younger learners and online safety campaigns
  - by pupils contributing to the writing and updating of the pupil AUA

c. Staff and volunteers

- All staff will receive online safety training and understand their responsibilities, as outlined in this policy.

- The OSL will receive regular updates through attendance at external training events (e.g. from the South West Grid for Learning (SWGfL)/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations
- The OSL will provide advice, guidance and training to individuals as required.
- Training to all staff will be offered as follows:
    - a planned programme of formal online safety and data protection training will be made available to all staff, which will be regularly updated and reinforced
    - an audit of the online safety training needs of all staff will be carried out regularly and individual requirements identified through their performance management
    - the training will be an integral part of the school's annual safeguarding and data protection training for all staff
    - training will include explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
    - all new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy and Acceptable Use Agreements/Code of Conduct
- Where staff are unsure of their responsibilities or recognise a lack of understanding and therefore a need for further training, they must raise this with their line manager..
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings and/or INSET days as required.

d. Governors

- Governors should take part in online safety training and awareness sessions, with particular importance for those who are members of any subcommittee or group involved in technology and online safety, health and safety and safeguarding. This may be offered in a number of ways:
    - attendance at training provided by the LA/MAT, National Governors Association or other relevant organisation (e.g. SWGfL)
    - participation in school training and information sessions for staff or parents, which may include attendance at assemblies and lessons
- A higher level of training will be made available to (at least) the Online Safety Governor

e. Parents

- Many parents 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 and regulation of the children's online behaviours. They 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 through:

- Regular communication, awareness raising and engagement on online safety issues, curriculum activities and reporting routes
- letters, newsletters, the school's web site and learning platform
- parents' information sessions through awareness workshops and parents' evenings etc, with the involvement of pupils where appropriate
- high profile events and campaigns e.g. Safer Internet Day
- reference to the relevant web sites and publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

8. Technology

The school is responsible for ensuring that its infrastructure and network are as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

a. Filtering

- The school's filtering procedures are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours.
- The school and tech support team manages access to content across its systems for all users through RM SafetyNet. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering .
- Access to online content and services is managed for all users.
- Illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- There are established and effective routes for users to report inappropriate content.
- There is a clear process in place to deal with requests for filtering changes.
- Filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
- If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.
- The school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
- Younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle, Google SafeSearch.
- Where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

b. Monitoring

- The school has monitoring systems in place to protect the school, systems and users:
  - the school monitors all network use across all its devices and services
  - an appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored and the OSL is responsible for managing the monitoring strategy and processes
  - there are effective protocols in place to report abuse/misuse and there is a clear process for prioritising response to alerts that require rapid safeguarding intervention
  - management of serious safeguarding alerts is consistent with safeguarding policy and practice
  - technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.
- The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school's risk assessment including:
  - physical monitoring (adult supervision in the classroom)
  - internet use is logged, regularly monitored and reviewed
  - filtering logs are regularly analysed and breaches are reported to senior leaders
  - pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
  - where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
  - use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

c. Technical security

- The 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 are securely located and physical access is restricted.
- There are rigorous and verified backup routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Online Safety Lead
- All school networks and systems will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by the school and the password must be changed to something secure.
- All users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security.

- The master account passwords for the school systems are kept in a secure place, e.g. school safe.
- Records of learner usernames and passwords for learners in Key Stage 1 or younger can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user and password requirements for learners at Key Stage 2 should increase as learners progress through school.
- xxxxxxxxxxx is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- Appropriate procedures, systems and security measures are in place:
  - for users to report any actual/potential technical incident or security breach
  - to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts, which might threaten the security of the school systems and data, which are regularly tested)
  - to protect the school's infrastructure and individual workstations with up-to-date endpoint (anti-virus software)
  - for the provision of temporary access of 'guests' (trainee/supply teachers and visitors) onto the school's system
  - regarding the personal use of school devices outside of school for all potential users
  - to prevent the authorised sharing of personal data unless safely encrypted or otherwise secured

d. Mobile technologies (including BYOD/BYOT[1])

- Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, wearable devices, 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.
- The school's acceptable use agreements for staff and volunteers, pupils and parents give clear guidance regarding the use of mobile technologies and these are attached as appendices to this policy.
- The school allows:

	School Devices		Personal Devices		
	School owned for individual use	**School owned for multiple users**	**Pupil owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network	*Yes*	*Yes*	*N/A*	*No*	*No*

[1] BYOD: bring your own device, BYOT: bring your own technology

access (filtered)					
Internet only	*N/A*	*N/A*	*N/A*	*Yes*	*Yes*

- All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational, irrespective of whether the device is school owned or personally owned.
- Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education and is consistent with and inter-related to other relevant school policies including but not limited to the Safeguarding and Child Protection Policy, The Behaviour Policy and Bullying Policy, the Staff Code of Conduct, Acceptable use agreements and policies around theft or malicious damage
- Pupils are not permitted to bring any of their own mobile devices into school, including mobile phones and wearable devices. If however they are required, mobile phones must be handed in to the school office or class teacher at the start of the day and collected once school has finished.

e. 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 and pupils need to be aware of the risks and legal implications associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place.

- The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.
- The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance.
- When using digital images, staff will inform and educate learners 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.
- Any images of pupils should only be taken on a school device. The personal device of staff/volunteers must not be used, except in an emergency, when such use must immediately be reported to a member of staff.
- Staff/volunteers must be aware of those learners whose images must not be taken/published and any images of pupils should
- In accordance with guidance from the Information Commissioner's Office (ICO), parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents comment on any activities involving other pupils in the digital/video images. This is clearly laid out in the acceptable use agreement for parents. However, there may be occasions where the school requests that parents

do not take pictures or videos, but this will only be done if felt absolutely necessary and the school requests that parents are supportive and comply with such requests.
- Staff and volunteers are allowed to take digital /video images to support educational aims, but must follow the school policies concerning the sharing, distribution and publication of those images.
- As required by the Data Protection Act, written permission from parents will be obtained before photographs of pupils are taken for use in school or published on the school website/social media. Parents will be informed of the purposes for the use of the images, how they will be stored and for how long, in line with Data Protection and Secure Data Handling procedures.
- Photographs published on the school website, or elsewhere, that include pupils will be carefully selected 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.
- Care will 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 into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission

f. Online publishing

- The school communicates with parents and the wider community and promotes the school through:
  - the school's website
  - social media
  - online newsletters
- The school website is hosted by PrimarySite and managed by school staff.

g. Data protection

- The school has a comprehensive 'Data Protection and Secure Data Handling Policy' written with reference to current legislation and guidance as issued by the Information Commissioner's Office, which clearly details the school's responsibilities and its staff.
- The school has appointed an appropriate Data Protection Officer who has an effective understanding of data protection law and is free from any conflict of interest.

10. Social media

a. School use:

- The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:
  - ensuring that personal information is not published

    - education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
    - clear reporting guidance, including responsibilities, procedures and sanctions
    - risk assessment, including legal risk
    - guidance for learners and parents
- School staff should ensure that:
    - no reference should be made in social media to learners, 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
    - they act as positive role models in their use of social media
- When official school social media accounts are established, there should be:
    - a process for approval by senior leaders
    - clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
    - a code of behaviour for users of the accounts (acceptable use agreements)
    - systems for reporting and dealing with abuse and misuse
    - understanding of how incidents may be dealt with under school disciplinary procedures.

b. Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, 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 personal social media sites during school hours

c. Monitoring of social media

- As part of active social media engagement, the school may 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
- When parents express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents should be informed of the school complaints procedure.

d. Cyberbullying[2] (including 'sexting'[3])

- Cyberbullying (including 'sexting')can be defined as "the use of technologies by an individual or group of people to deliberately and repeatedly upset someone else"[4]
- For most, using the internet and mobile devices is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that young people, school staff and parents understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.
- Cyberbullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school's Behaviour, Anti-Bullying and Safeguarding and Child Protection policies, which include:
  - clear procedures set out to investigate incidents or allegations of cyber bullying
  - clear procedures in place to support anyone in the school community affected by cyber bullying
- All incidents of cyberbullying reported to the school will be recorded.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the ISP and the police, if necessary.
- Pupils, staff and parents will be required to work with the school to support the approach to cyberbullying and the school's e-safety ethos.
- Further guidance and advice regarding 'sexting' can also be found through the following links:
  - UKCIS 'Advice for schools: Responding to and managing sexting incidents')
  - DfE December 2020 - Sharing nudes and semi-nudes: how to respond to an incident (overview)

11. Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

---

[2] Childnet.com: 'Understanding cyberbullying'

[3] Sexual violence and sexual harassment between children in schools and colleges (DfE 09/21)

[4]

12. Handling of complaints

- Parents and pupils will need to work in partnership with the school to resolve issues.
- Where complaints do not involve acts which are clearly illegal (e.g. accessing child abuse images or distributing racist material) they should be dealt with through the school's normal complaints procedures as outlined in the school's Complaints Policy.
- Complaints regarding Illegal activity would be dealt with in line with the school's safeguarding and disciplinary procedures and where required, would involve contact with the police and could lead to criminal prosecution, as could clear cases of cyberbullying.
- As detailed above, there are clear procedures in place to deal with concerns around cyberbullying and such incidences should be brought to the attention of the school as early as possible.
- Any complaint about staff misuse must be referred to the Headteacher.
- Any complaint about the Headteacher/Principal should be referred to the Chair of Governors.
- Where any member of the school community has breached the terms of their respective 'Acceptable Use Agreement', the school reserves the right to restrict their access to the school's internet.

13. Relevant policies

This policy should be read and understood in conjunction with the following documents:

- Acceptable Use Agreements
- Anti-bulling Policy
- Behaviour Policy
- Child Protection Policy
- Data Protection and Secure Data Handling Policy
- Good Practice Guide for Volunteers and External Agency representatives working in school
- Remote Learning Policy
- Social Networking Policy (WSCB)
- Staff Code of Conduct
- Guidance for Safer Working Practice for Adults working with Children and Young People (February 2022)
- Keeping Children Safe in Education (DfE)
- Screening, Searching and Confiscation at schools (DfE 09/22)
- Education for a Connected World framework (UK Council for Internet Safety 2020 Edition)
- Teaching online safety in schools (DfE Published January 2023)
- Teachers' Professional Standards (DfE Updated December 2021)
- SWGfL Project Evolve – online safety curriculum programme and resources

APPENDICES

1	**Staff and Volunteer Acceptable Use Agreement**
2	**Pupil Acceptable Use Agreement (EYFS and KS1)**
3	**Pupil Acceptable Use Agreement (KS2)**
4	**Online Safety Incident Flow chart**
5	**Procedures to handle incidents of misuse, including responding to illegal incidences (flow chart)**

Staff and Volunteer Acceptable Use Policy

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

This Acceptable Use Policy is intended to ensure:

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

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students/pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school may monitor my use of the ICT systems, email and other digital communications.

- I understand that the rules set out in this agreement also apply to the use of school ICT systems (e.g. laptops, email, VLE etc) out of school.

- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner. Further to this I will never give out my personal address, mobile phone number etc or that of other members of the staff/school community without their express permission.
- I will not engage in any online activity either at home or in school that may compromise my professional responsibilities including but not limited to using social networking sites to discuss grievances relating to work or children, members of staff, comments, confidential matters or any activity that may bring the school into disrepute.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal handheld/external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow

any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.

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

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

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that I am responsible for my actions in and out of school.
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school but also applies to my use of school ICT

systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority, dismissal and in the event of illegal activities the involvement of the police.

EYFS and Key Stage 1 Acceptable Use Agreement

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 the computer 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

Key Stage 2 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 my username and password 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 (eg YouTube), unless I have permission of a member of staff to do so.

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:

- If I bring in a mobile phone, I will hand it in to the office at the beginning of the school day.

- 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 not access social media sites or applications unless given permission.
-

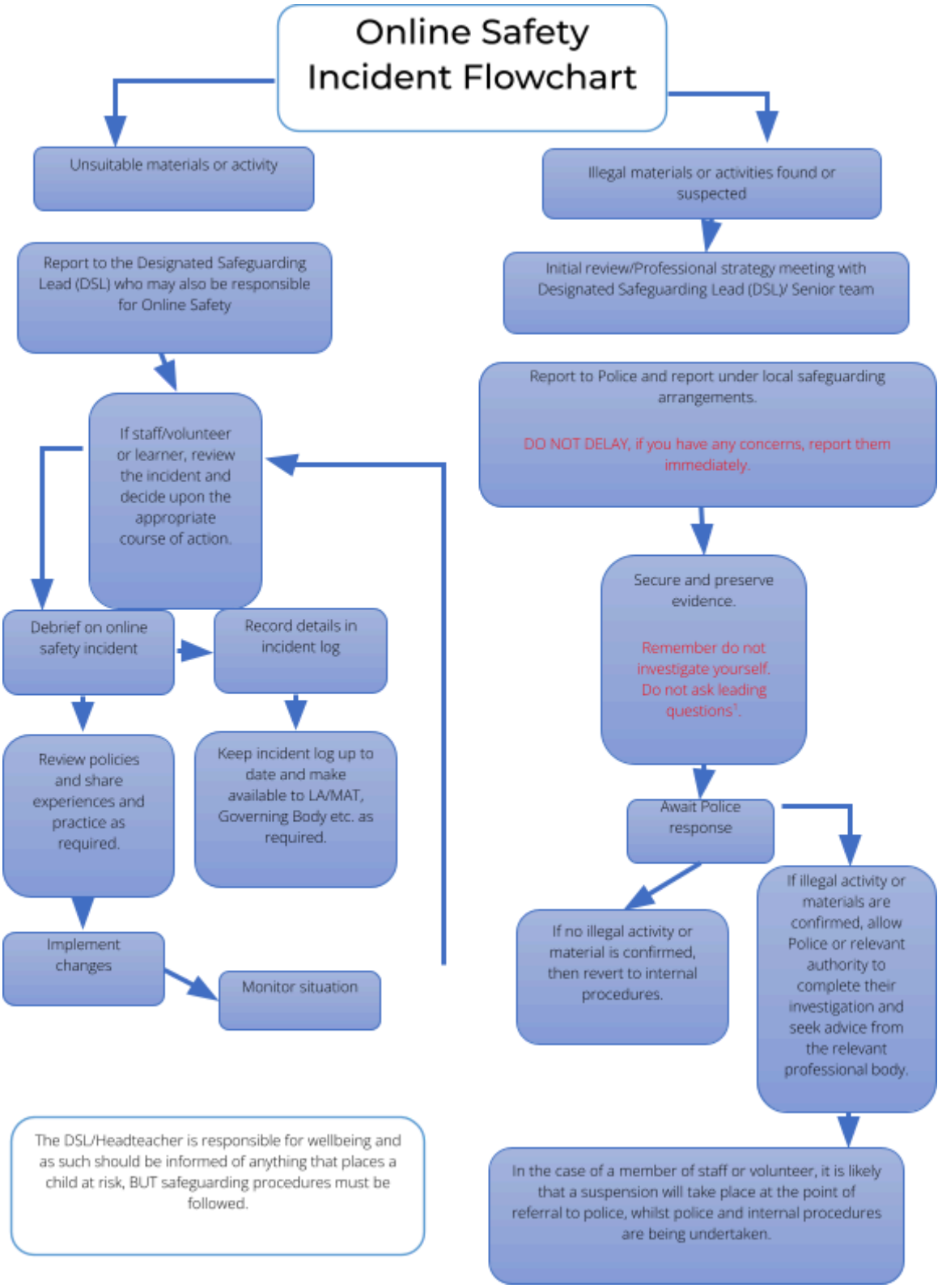
When using the internet for research or recreation, I recognise that:

- 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.

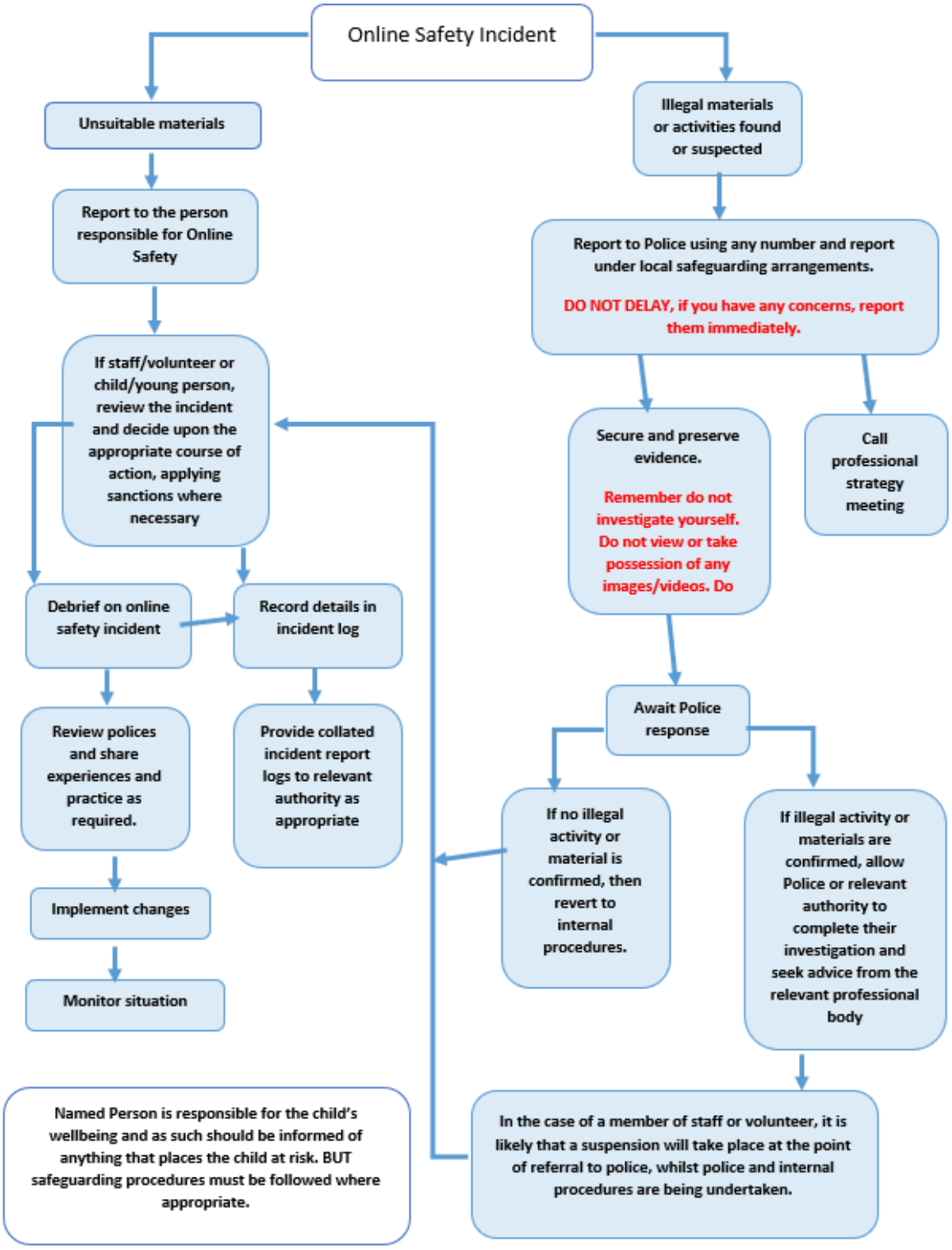
I understand that I am responsible for my actions, both in and out of school:

- 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 cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, stages, suspensions, contact with parents and in the event of illegal activities involvement of the police.

ONLINE SAFETY POLICY APPENDIX 4 - Online Safety Incident Flowchart



ONLINE SAFETY POLICY APPENDIX 5 - Procedures to handle incidents of misuse, including responding to illegal incidences



*Chair of Governors to be involved if there is a significant incident regarding a staff member.