St. James' Blackburn CE Primary School

Vision Statement

Guided by our Christian Values, we endeavour to inspire, cherish and serve our school community. We strive to be exceptional in all we do. We will nurture a love of all God's children. We seek to build respect for all faiths and beliefs.

'Serve one another in love' (Galatians 5.13)

Mission Statement

Together we value, inspire and develop each other within a happy, safe community based on Christian values and respect for other faiths.

'Show respect to everyone' (Peter 1 2.17)

LOVE

'Serve one another in love' (Galatians 5.13)

RESPECT

'Show respect to everyone' (Peter 1 2.17)

COURAGE

'Be strong and courageous; do not be frightened or dismayed, for the Lord your God is with you wherever you go.' (Joshua 1.9)

Online Safety Policy

Date reviewed by school: 15/12/2023

Next review date: 01/12/2026

School Vision
Guided by our Christian Values we endeavour to inspire, cherish and serve our school community. We strive to be exceptional in all we do. We will nurture a love of all God's children. We seek to build respect for all faiths and beliefs.

'Serve one another in love' (Galatians 5.13)

School Mission Statement

Together we value, inspire and develop each other within a happy, safe community based on Christian values and respect for other faiths.

'Show respect to everyone' (Peter 1 2.17)

School Values
The school has 9 school values underpinned by 3 core Christian Values of:

Courage
'Be strong and courageous; do not be frightened or dismayed, for the Lord your God is with you wherever you go.' (Joshua 1.9)
Love
'Serve one another in love' (Galatians 5.13)
Respect
'Show respect to everyone' (Peter 1 2.17)

At St James' Church of England Primary School, we strive to be exceptional in all that we do and ensure that the curriculum and its delivery reflect this vision. We are committed to high quality teaching and learning to raise standards of achievement for all pupils.

Staff have been consulted in developing this policy, which summarises expectations and common working practices. It reflects what has been agreed in terms of approach and consistency and makes explicit the exceptional practice to which the school aspires. It also reflects the mission and values of the school and supports its vision.

This Online Safety Policy has been written by the school, building on the Blackburn with Darwen policy that has been adapted from Kent County Council/The Education People Online Safety Policy template 2018 and the SWGfl template in line with the Online 360 review tool. It has been agreed by the Senior Leadership Team and approved by Governors.

SWGfL/UK Safer Internet Centre -The South West Grid for Learning Trust is an educational trust with an international reputation for supporting schools with online safety.

SWGfL, along with partners Childnet and IWF, launched the UK Safer Internet Centre (UKSIC) in January 2011 as part of the European Commission's Safer Internet Programme. The Safer Internet Centre is, for example, responsible for the organisation of Safer Internet Day each February. More information about UKSIC services and resources can be found on the website: www.saferinternet.org.uk. SWGfL is a founding member of UKCIS (UK Council for Internet Safety). It has contributed to conferences across the world and has worked with government and other agencies in many countries. More information about its wide-ranging online safety services for schools can be found on the SWGfL website – swgfl.org.uk

Writing and reviewing the Online Safety policy

The Online Safety Policy relates to other policies including those for Computing, bullying and for child protection. It has been developed through consultation with various stakeholders at St James' CE Primary made up of:

- Head teacher and senior leaders
- Online Safety Coordinator
- Staff – including teachers, support staff, admin and technical staff
- Governors
- Children and families

Consultation with the whole school has taken place through a range of formal and informal meetings.

- The schools Online Safety Co-ordinator works in collaboration with the Designated Safeguarding Lead (DSL).
- The Online Safety Policy and its implementation will be reviewed annually or in response to an incident.
- The Online Safety Policy was revised by DSL

School uses '360-degree safe Online Safety Self Review Tool'

360 degree safe is an online, interactive self-review tool which allows school to review the online safety policy and practice. It is free of charge - with over 10,000 registrations, since its introduction in 2009. The tool provides an "improvement action". School can use the tool to compare its levels to the average levels of all the schools/academies using the tool and to the Online Safety Mark benchmark levels. There is a range of reports that they can use internally or with consultants.

The tool suggests possible sources of evidence, provides additional resources/good practice guidance and collates the school's action plan for improvement.

Schools that reach required benchmark levels can apply for assessment for the Online Safety Mark, involving a half day visit from an accredited assessor who validates the school's self-review.

Staying safe

The school will ensure that pupils and parents are aware of Online safety issues. A list of useful addresses and resources are included in this document.

- The school internet access is designed for pupil use and includes appropriate filtering.

- Pupils may only use approved digital methods of communication on the school system for educational purposes.
- Pupils will be taught to tell an adult immediately about any offensive communications they receive or any inappropriate content they may encounter using digital technology.
- Pupils and staff will use setting owned equipment in accordance with our acceptable use policies.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location or arrange to meet anyone without specific permission.
- Pupils and parents will be advised that the unsupervised use of age restricted social network spaces outside school is inappropriate for pupils.

Safety Audit

The self-audit assesses whether the Online Safety basics are in place to support a range of activities.

Has the school an Online Safety Policy that complies with Becta guidance?	Yes
Date of latest update: Autumn 2023	
The Policy was first agreed by governors on: Autumn 2022	
The Designated Leads for Child Protection are : V Moore S Rehman	
The Online Safety Co-ordinator is: C Forshaw	
Has Online Safety training been provided for both students and staff?	Yes
Do all staff sign a digital technology system (Acceptable Use and Code of Conduct) on appointment?	Yes
Do parents sign and return an agreement that their child will comply with the School Online Safety Rules?	Yes
Have school Online Safety Rules been set for pupils?	Yes
Are these Rules displayed in all rooms with computers?	Yes
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access	Yes
Has a digital technology systems security audit been initiated by SLT, possibly using external expertise	Yes
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Yes

Authorising Internet access

- All staff must read and sign the 'Acceptable use and Code of Conduct,' before using any school technology.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave.
- Parents will be asked to sign and return a consent form when borrowing school equipment.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Blackburn with Darwen LA can accept liability for the material accessed, or any consequences of Internet access. Any inappropriate access whether intentional or unintentional will be reported to the Online Safety Co-ordinator, DSL and to the LA where necessary.
- The school will audit digital technology systems provision to establish if the Online Safety policy is adequate and that its implementation is effective.

Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and where appropriate inform the LA.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaint's procedure available on the school website.

The school will monitor the impact of the policy using:

- Logs of reported incidents (CPOMS)
- Monitoring logs of internet activity (including sites visited/filtering)
- Internal monitoring data for network activity
- Surveys/questionnaires of
    - pupils
    - parents/carers
    - staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers 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 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. In the case of both acts, action can only be taken over issues covered by the published Behaviour and Rewards 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

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 has taken on the role of Safeguarding including Online Safety. The role may include:

- regular meetings with the Online Safety Co-ordinator

- possible attendance at Online Safety meetings
- regular monitoring of online safety incidents
- regular monitoring of filtering logs
- reporting to relevant Governors meetings

Head teacher and Senior Leaders

- The Head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Head teacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Head teacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head teacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

- Leads the Online Safety Champions
- 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 SLT and possibly the Local Authority
- Liaises with school technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- Meets with Safeguarding/Online Safety Governor to discuss current issues, review incident logs and filtering logs
- Attends relevant meetings of Governors
- Reports regularly to Senior Leadership Team

Network Manager/Technical staff

Those with technical responsibilities are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online safety technical requirements and any Local Authority/ other relevant body 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 (installed on network) 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 Head teacher and Senior Leaders; Online Safety Lead 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/Code of Conduct agreement
- They report any suspected misuse or problem to the Head teacher/Senior Leader/Online Safety Lead for investigation/action/sanction
- All digital communications with 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
- Pupils understand and follow the Online Safety Policy
- Upper Key Stage 2 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 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

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Online Safety Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (upper KS2)
- 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.

- Designated 'Online Safety Champions' are responsible for promote Online Safety throughout school

Parents/carers

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

- Digital and video images taken at school events
- Access to parents' sections of the website/Learning Platforms
- Their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems or programmes as part of the wider school provision will be expected to sign an acceptable use agreement before being provided with access to school systems.

Policy Statements – Teaching and Learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Education – 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/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.
In planning online safety curriculum, the following documents have been used:

- DfE Teaching Online Safety in Schools
- Education for a Connected Word Framework
- SWGfL Project Evolve – online safety curriculum programme and resources
- Google Internet Legends

As the children's access and understanding expands, so should the guidance and rules to ensure safe access use of the internet

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
- 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.

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- 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 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.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will contribute to and follow age appropriate Online Safety Rules.
- Pupils will be taught what responsible Internet use is and what is not and given clear objectives for Internet use.
- Pupils will be taught how to evaluate Internet content appropriate to their age.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation appropriate to their age group.
- Sanctions for inappropriate use of the internet will be explained to the children.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Where 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, pupils 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 will therefore seek to provide information and awareness to parents and carers through:

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

Education – The Wider Community

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

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

Education & Training – Staff

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 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 (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Training – Governors

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. And understand the schools filtering and monitoring IT systems. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or National Governors Association or another relevant organisation (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents.
- Monitoring visits and meetings with the DSL and Online Safety Lead.

Technical – infrastructure/equipment, filtering and monitoring

School will follow the DFE publication of filtering and monitoring standards and guidance. The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

Managing Internet Access

Our filtering system should block harmful and inappropriate content without reasonably impacting on teaching and learning.

Information system security

- 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
- Security strategies will be discussed with Blackburn with Darwen.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All adult users (and upper KS2 pupils) will be provided with a username and secure password Technical staff, who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master/administrator" passwords for the school systems, used by the Network Manager (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place (e.g. school safe)

Technicians are 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

Managing filtering

- The school will work with the LA and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Coordinator or DSL and the LA will be informed so that they can take appropriate action.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. (There is a clear process in place to deal with requests for filtering changes
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place (big red button) for pupils to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images - Published content

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:

Any information that can be accessed outside the school's intranet should be classed as published whether in electronic or paper format.

- Electronic communication sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- General contact details should be the school address, e-mail and telephone number.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- When using digital images, staff should inform and educate 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 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 events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school 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 into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Managing emerging technologies

- The educational benefit of emerging technologies and any potential risks will be considered before it is used in school.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and General Data Protection Regulations (GDPR).

Communications

Introducing the Online Safety policy to pupils

- Online Safety rules are regularly updated in collaboration with the 'Online Safety Champions' and online posters. The rules will be posted in all classrooms and discussed regularly with the pupils.

Staff and the Online Safety policy

- All staff will be given the School Online Safety Policy and its importance explained.
- Staff should be aware that internet traffic may be monitored and traced to the individual device or login. Discretion and professional conduct is essential.
- The school may use monitoring software where this is available to ensure that inappropriate materials are not being stored or used on school equipment.

Enlisting parents' support

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and on the school website.
- Parents agree to Online Safety Agreement when starting.

Use of Communications Technologies

A wide range of rapidly developing communications technologies has the potential to enhance learning. School carefully considers the benefit of using these technologies for education alongside their risks/disadvantages.

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

- Whole class/group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- 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.
- Staff should also refer to the Staff Code of Conduct.

Dealing with unsuitable/inappropriate activities

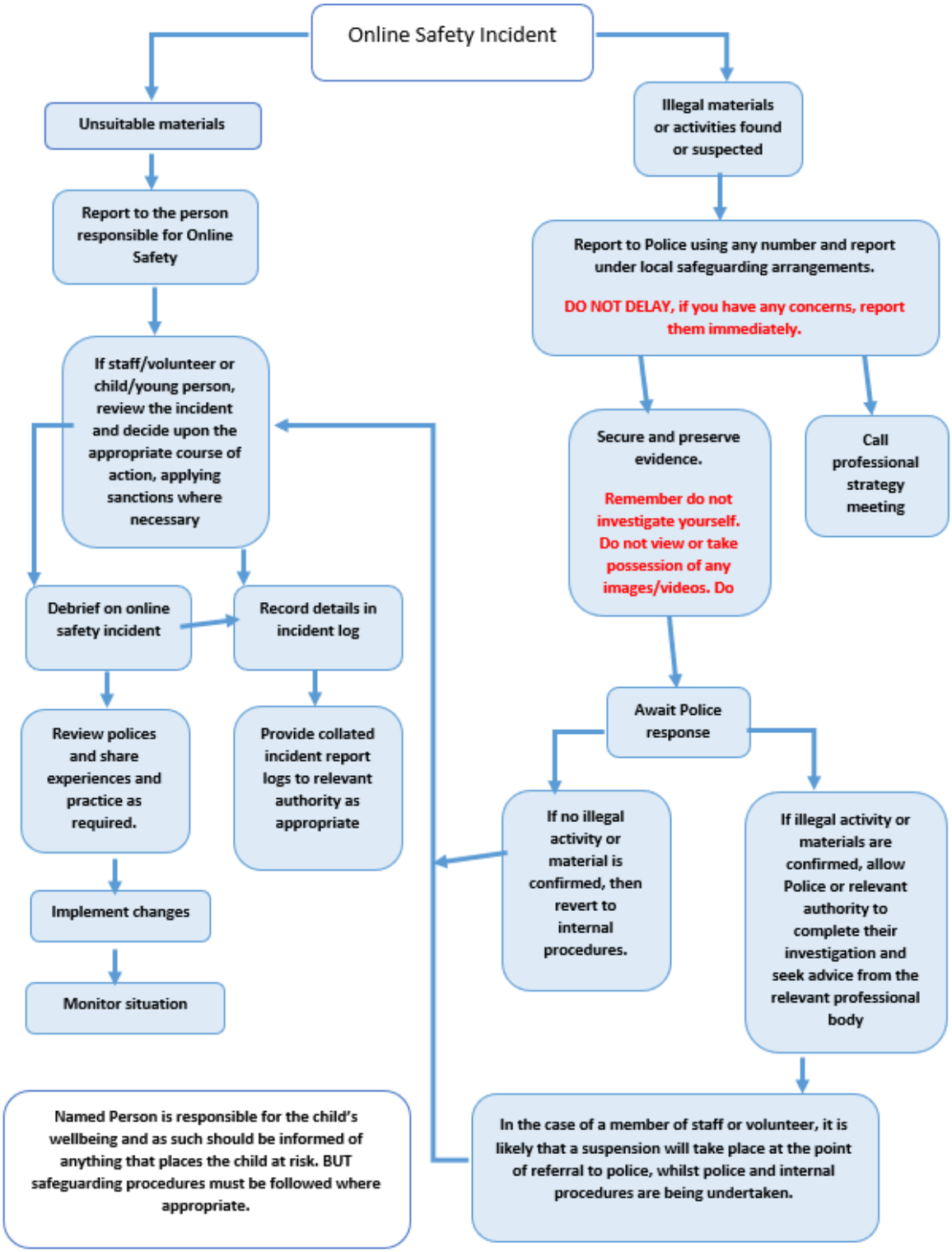
Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities 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.

Responding to incidents of misuse

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

Illegal Incidents

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



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school 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 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 safeguarding/behaviour/disciplinary procedures.

Appendix

Useful addresses

Safer Internet Centre Professional helpline
http://www.saferinternet.org.uk/about/helpline
CEOP videos
http://www.thinkuknow.co.uk
Digital parenting magazine
http://www.parentzone.org.uk
Internet matters
http://internetmatters.org
UK Safer Internet Centre
http://saferinternet.org.uk
Google Internet Legends
https://beinternetawesome.withgoogle.com/en_uk/

Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework