The Policy and Procedures for Online Safety

Our school helps us to walk with Jesus to be the best that we can be. Through God's love and guidance, we create an ethos of shared endeavour, friendship and co-operation to help us flourish academically, emotionally and spiritually.

"I can do all things through Christ, who strengthens me."
Philippians 4:13

Policy Author	Mrs Julie Green
Policy Date	September 2022
Approved by Governors	November 2022
Next Review	September 2023

Table of Contents

Introduction	3
Schedule for Review	3
Roles and Responsibilities	4
Intent	8
Implement:	
Pupils	8
Parents and Carers	9
Staff and Volunteers	9
Governors	9
Technical:	
Mobile Technologies	11
Filtering	12
Digital and Video Images	13
Data Protection	14
Communications and Social Media	15
Child on Child Abuse	17
Responding to Online Safety Concerns	18
Responding to Incidents of Misuse	18
Responding to Incidents of Cyberbullying	18
Illegal Incidents	20
External Links	21
Appendix	22

Introduction

Children and young people today are using digital media to explore, connect, create, and learn in ways never before imagined. However, alongside these new experiences and opportunities, children can become exposed to potential risks. It is vital therefore that schools endeavour to teach children and young people to learn digital literacy and citizenship skills so that they can act responsibly and to use the internet in a better way.

Online safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. The school's online safety policy will operate in conjunction with *'Keeping Children Safe in Education 2019'* and other policies including those for *Safeguarding, Behaviour, Anti-Bullying, Curriculum* and *Data Protection.*

This Online Safety policy has been developed by the school's Online Safety Group which consists of:

- Mrs Julie Green – Head Teacher/Designated Safeguarding Lead
- Miss Charlotte McCormack – Deputy Head Teacher/Deputy Designated Safeguarding Lead
- Mrs Julie Green – Online Safety Lead/Computing Lead
- Mr Jerard Knott – Chair of Governors
- Mr Jerard Knott – Assigned governor for Computing and Online Safety

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

Schedule for Review

This Online Safety policy was approved by the Governing Body on:	*November 2022*
The implementation of this Online Safety policy will be monitored by the:	*Online Safety Committee outlined above*
Monitoring will take place at regular intervals:	*Annually or when requested*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies. The next anticipated review date will be:	*September 2023*
Where an online safety breech occurs, we will approach the appropriate external agency. This will depend on the circumstances and may include:	*MASH, Police, Lancashire Safeguarding, County Advisor, Children and Family Well-Being Services*

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

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 annually, with governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body (Jerard Knott) has the role of Online Safety Governor.

The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Lead
- attendance at Online Safety Group meetings
- regular and pro-active monitoring of:
  1) online safety incident logs
  2) filtering control logs
- reporting to relevant staff members and stakeholders

Head Teacher

- The Head teacher (Mrs Julie Green) has a duty of care for ensuring the safety (including online safety) of members of the school community, and the day-to-day responsibility for online safety will be delegated to the Online Safety Lead (from September 2022 until further notice this will be Mrs J Green)
- The Head teacher and Deputy Head teacher are 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, where relevant.
- The Head teacher also liaises with the Local Authority and relevant body

Online Safety Lead

The Online Lead (Mrs J Green):

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy.
- 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 school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- meets regularly with Online Safety Governor to discuss current issues and review incident logs and filtering
- attends relevant meetings of Governors to report back on any arising issues
- ensures the use of the internet is monitored and reports and incidents to the relevant persons

Technical Staff

The Network Manager (Blue Rock IT Services) is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets at least the minimum required online safety technical requirements and any local authority guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy, *Netsweeper*, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

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 Policy (AUP)
- they report any suspected misuse or problem to the Head teacher and Online Safety Lead for investigation
- 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 acceptable use agreement

- 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, and mobile devices (iPads and laptops) 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 processes should be in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead (including Deputy)

Will 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

Online Safety Group

The Online Safety Group is made of members of the school community with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including its impact. Members of the Online Safety Group will assist the Online Safety Lead (or other relevant person, as above) with:

- the production/review/monitoring of the school Online Safety Policy
- monitoring of the school filtering policy and requests for filtering changes
- mapping and reviewing the online safety provision – ensuring relevance, breadth and progression
- monitoring incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the online safety provision

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- will be expected to know and understand policies on the use of mobile devices (iPads, laptops, digital cameras, smart watches.) 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 Acceptable Use Agreement covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through annual parent workshops, monthly newsletters and information regarding current issues. Parents and carers are 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 and the school Facebook page

Online Safety Intent at Baxenden

In a world in which the internet has become a pivotal aspect of children's lives, our online safety curriculum provides our pupils with the necessary skills to become safe, positive and conscientious users of the digital world.

Implement

Implement refers to the way our curriculum is taught and organised, including how we achieve our intent at Baxenden.

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

Online safety is a focus in all areas of the curriculum and all school staff have a duty to reinforce online safety messages across the curriculum. The school currently use Rising Stars Online Safety to provide a broad, relevant curriculum, which provides progression, with opportunities for creative activities and this is provided in the following ways:

- Online Safety lessons, linked to the Rising Stars curriculum, are taught as part of Computing units
- A stand-alone lesson on online safety begins each unit in a half-term and is then reinforced throughout the work in that unit
- All pupils begin the school year by signing the Pupil Acceptable Use policy, which is discussed in detail
- Key online safety messages are reinforced through assemblies and pastoral activities
- In all lessons where the internet is used, pupils are taught and reminded to be critically aware of the materials and content they access online and are guided to validate the accuracy of information
- Pupils are taught to acknowledge the source of information and to respect copyright when using material accessed on the internet
- Where an incident occurs or arises, pupils are referred to the Acceptable Use Policy and any other relevant policies in order to consider their actions and the actions of others
- All pupils from Year 1 – Year 6 receive an annual Online Safety Workshop (usually with a trained Lancashire Online Safety Advisor)
- All pupils participate in Safer Internet Day every February

Parents and Carers

Parents and carers play an essential role in the education of their children and in the monitoring and 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 provide information and awareness to parents and carers through:

- Monthly newsletters regarding current issues and updates
- An annual parent workshop provided by a Lancashire Online Safety Advisor or a member of the online safety team
- The use of the school Facebook page to raise awareness of any additional information which needs to be shared
- Sending out information regarding UK Safer Internet Day
- Making reference and providing links to relevant websites and documentation in the Online Safety section of the school's website

Staff and Volunteers

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

- A planned cycle of online safety training, which is completed annually with all members of staff
- All new staff receive online safety training and are directed to the school's Online Safety Policy and Acceptable Use Policy as part of their induction process
- The Online Safety Lead and other members of the Online Safety Group attend regular networks and relevant external training courses, feeding back to other staff where necessary
- The Online Safety policy and its updates are presented to and discussed with staff regularly

Governors

Governors take part in online safety training, with particular importance for those who are members of any subcommittee or group involved in technology/online safety/health and safety and safeguarding. This is offered through:

- Attendance at training provided by the Local Authority
- Participation in school training and information sessions for staff or parents, including attendance at relevant worships and lessons

Home Learning Platforms

In light of the Covid-19 pandemic, many of our children had to learn from home over a prolonged period of time. We have been able to deliver high-quality teaching and learning via the online platform Seesaw. This has played a key role in ensuring that all pupils remain as unaffected as possible whilst not being able to attend school.

Seesaw will continue to play an important part in our school curriculum and will continue to provide lessons for those unable to attend school. Parents and pupils have been made aware of our expectations when signing our 'Home School Agreement' this can be found in the appendices.

Technology

Mobile Technologies

Mobile technology devices may be school-owned, provided or personally owned and might include: smartphone, tablet, notebook, laptop, smartwatch or other technology that usually has the capability of utilising the school's wireless network and using digital images. The device then has access to the wider internet which may include cloud-based services such as email and data storage.

The school currently has 41 iPads, which consist of 8 staff iPads and 33 pupil iPads. These are currently split over both key stages, 21 in KS2 and 12 in KS1. iPads are used to support learning in a variety of areas including:

- Searching the internet for a research-based lesson
- Various learning apps, most predominantly Active Learn, My Maths and Times Tables Rockstars
- Recording apps including Pic Collage and Popplet
- Evidencing learning through digital photos and videos

The school also has a media suite which houses 22 pupil computers and 12 laptops for use in lessons. Additionally, each classroom contains a teacher laptop and KS1 classrooms house 4 pupil computers per classroom. Laptops are also used in the school hall, offices and staff meeting room.

All laptops and iPads used in school have been authorised by the Head teacher for educational purposes and run on the school's network. Each user has an individual login and password, which is updated regularly to prevent password misuse and protect data.

All users, including the pupils, sign an Acceptable Use Policy and understand that the primary purpose of the use of mobile or personal devices in a school context is educational. The expected and accepted use of mobile technologies is outlined in the table on the following page.

	School Devices			Personal Devices		
	School owned for single user e.g. teacher computer /laptop	**School owned for multiple users e.g. pupil computers and laptops, IPads**	**Authorised device (authorised only by the Head teacher or the Online Safety Lead)**	**Pupil owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes**	*Yes***	*Yes*
Full network access	*Yes*		*Yes*			
Internet only		*Yes*				
No network access				*Yes*	*Yes*	*Yes*

**A pupil-owned device is only allowed in school where staff have been informed and the pupil has been given permission. The device must be switched off, handed into the school office at the beginning of the school day and collected at the end of the school day. This includes all personal devices listed on page 11.*
*** All staff sign an Acceptable Use Policy which states that personal devices are only to be used at certain times of the day. For example, lunchtime, and must not be used in view of the children or to take photos/videos of the children. This is also the case for external visitors.*

Filtering

The school will work with the Local Authority and the Internet Service Provider to ensure systems to protect and safeguard children are reviewed and improved. The school deploys the Local Authority filtering system in school – Netsweeper. The settings are managed by Blue Rock IT Services and the Online Safety Lead – these are in line with authority guidance. If staff or pupils come across unsuitable online materials, the site must be reported to the Online Safety Lead. Any issues or suspicious activity will be investigated by the SLT/Governing body to ensure children are safeguarded.

Parents will be advised upon the importance of filtering on home computers via the school website and/or Online Safety workshops.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, all parties involved need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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. To reduce the likelihood of the potential for harm, the school will inform and educate users about these risks and will implement policies:

- When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. This is included in the Rising Stars Online Safety scheme that the school follows to support the curriculum. 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 platforms or in the local press
- Parents and carers are informed at the start of any school event if they are unable to take videos and digital images. To respect everyone's privacy and in some cases protection, where images and videos are permitted to be taken, these images should not be published on social networking sites (other than the school run and approved sites), nor should parents or carers comment on any activities involving other pupils in the content
- Staff and volunteers are allowed to take digital video or images to support educational aims, but this must be done on authorised devices and they must follow school policies concerning the sharing, distribution and publication of those images
- 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.
- Where pupils' full names are used on a website or blog, they will not be used in association with photographs.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Please see the *Data Protection Policy* for more information.

The school:

- Has a Data Protection Policy.
- Has paid the appropriate fee to the Information Commissioner's Office (ICO).
- Has appointed a Data Protection Officer (School Business Manager.)
- Will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. This data must be accurate and updated regularly.
- Has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Has clear and understood methods of data retention and routines for the deletion and disposal of data.
- Considers the protection of personal data when accessed using any remote access solutions.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

Communications and Social Media

Communications

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

- The official school email service is regarded as safe and secure and is used only for communications which are relevant to their job role
- Users must immediately report, to the nominated person the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff, pupils, parents and carers (email, social media etc) must remain professional and only take place using authorised school systems
- Pupils will be taught about the risks attached various methods of digital communication as part of the Online Safety Scheme of work and Computing curriculum
- Staff email addresses remain hidden from parents – only a bursar and head email address is made available on the school website
- In computing units where email is used, the pupils will use Seesaw as a secure platform for communicating
- Teachers are able to communicate with parents via Seesaw to communicate any issues or announcements both individually and collectively

Social Media

As part of ongoing communications, the school uses a Facebook page and a Twitter Account. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school on these platforms through:

- Ensuring that personal information is not published
- Training is provided annually including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions, including the possibility of disciplinary action
- Ensuring a process for approval by senior leaders
- The accounts are managed only by appointed staff

School staff ensure that:

- They do not engage in online discussion on personal matters relating to members of the school community

- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined system or process

Child on Child Abuse

It is important to recognise that children can abuse other children and it can happen both inside and outside of educational settings and online. This is referred to as **'child on child abuse**' and can include:

- bullying, including cyberbullying, prejudice-based and discriminatory bullying
- abuse in intimate personal relationships between children and peers
- physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm; this may include an online element which facilitates, threatens and/or encourages physical abuse
- sexual violence; this may include an online element which facilitates, threatens and/or encourages sexual violence
- sexual harassment, such as sexual comments, remarks, jokes and online sexual harassment, which may be standalone or part of a broader pattern of abuse
- causing someone to engage in sexual activity without consent
- consensual and non-consensual sharing of nude and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery)
- 'Upskirting' which involves taking a picture under someone's clothing without them knowing causing the victim humiliation, distress or alarm. 'Upskirting' is a criminal offence and anyone of any gender, can be a victim

All staff at Baxenden are able to recognise the indicators and signs of **child-on-child abuse** and know how to identify it and respond to reports in line with the safeguarding and child protection policy. Even if there are no reports of **child-on-child abuse**, it is recognised by staff that this does not mean it is not happening; it may be the case that it is just not being reported.

Staff at Baxenden understand the importance of challenging inappropriate behaviours between children that are actually abusive in nature. Downplaying certain behaviours, for example dismissing sexual harassment as "banter", "just having a laugh", "part of growing up" or "boys being boys" can lead to a culture of unacceptable behaviours, an unsafe environment for children and in worst case scenarios, a culture that normalises abuse leading to children accepting it as normal and not coming forward to report it.

Stopping violence and ensuring immediate physical safety is a school's first priority but emotional bullying can be more damaging than physical; teachers and schools have to make their own judgements about each specific case.

Bullying type behaviour also includes where there is an imbalance of power, leaving the person who is being bullied feeling defenseless.

Bullying may be carried out by an individual pupil or groups of pupils, by an unknown person or group, and is made up of repeated/regular incidents.

Responding to Online Safety Concerns

As part of ongoing child protection, the school uses CPOMS as a method of reporting concerns and incidents related to online safety. Notification of these concerns are sent directly to the senior leadership team (SLT), recorded in the online safety concern chronology and dealt with in accordance with child protection procedures (see Child Protection policy.)

Where relevant, other parties such as parents, carers and external agencies may be contacted.
Where a member of staff or the wider community has an online safety concern regarding a member of staff, these should be reported to the Head teacher or Chair of Governors and will be investigated and dealt with immediately.

Responding to Incidents of Misuse

Any incidents of misuse, both in or out of school, are reported directly to the SLT and dealt with immediately. When the incident has taken place in school, the pupil or pupils in question will have their internet access removed in accordance with the Acceptable Use Policy and parents/carers will be contacted. In the event that misuse has been identified in a member of staff, this will result in disciplinary action.

Any incident which has occurred outside of school will be investigated and referred to parents, carers or the police where necessary. School will provide support and guidance to the best of its ability in these instances and continue to closely monitor the pupil's use of the internet within school.

Responding to Incidents of Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. There are clear procedures in place to support anyone in the school community affected by cyberbullying and all incidents of cyberbullying reported to the school will be recorded on a bullying concern log in accordance with the Anti-Bullying policy. There are clear procedures in place to investigate incidents or allegations of Cyberbullying:

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate, which may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's online safety intent

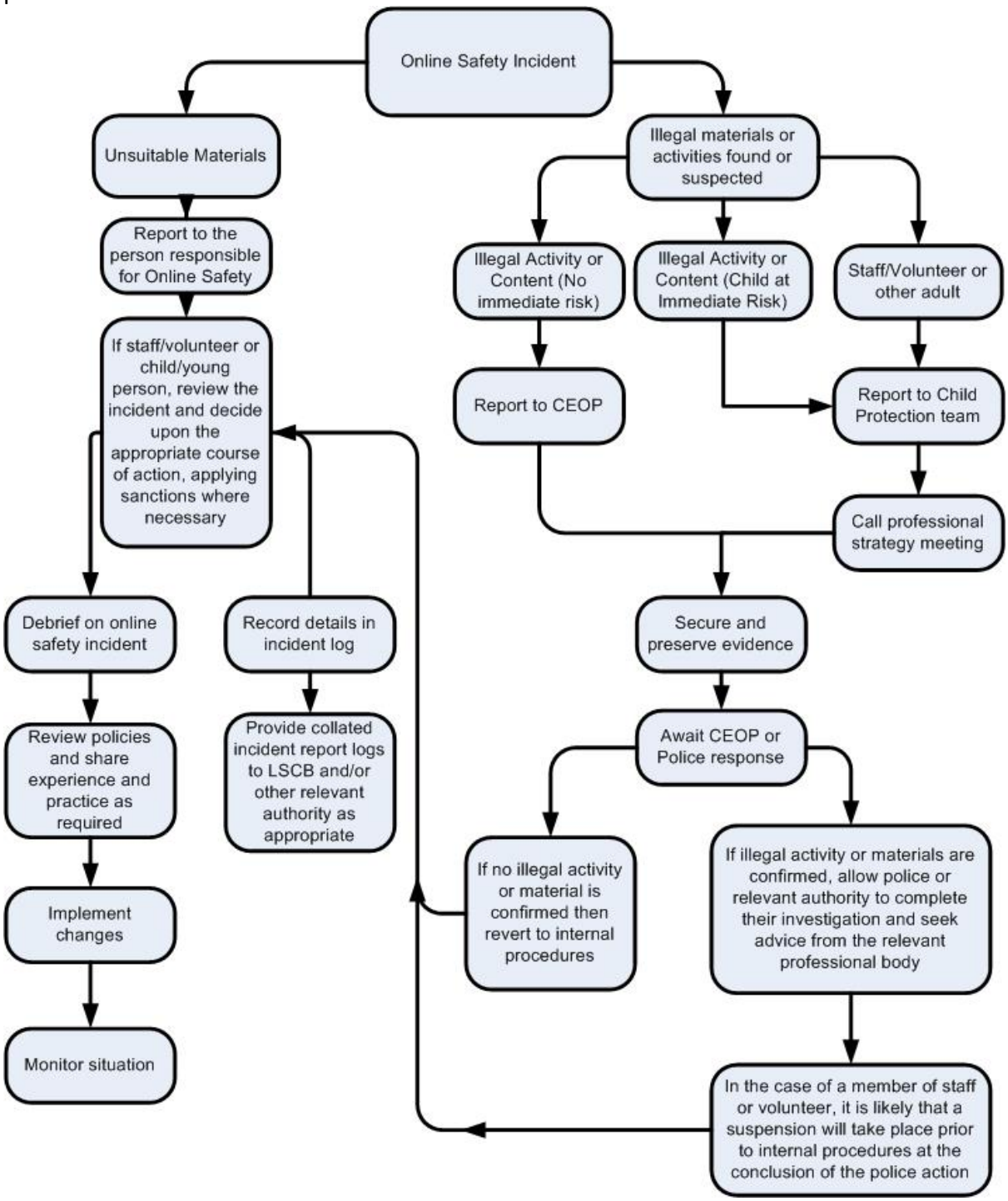
Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content

- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti bullying, behaviour policy or Acceptable Use Policy
- Parent/carers of pupils will be informed
- The Police will be contacted if a criminal offence is suspected

Illegal Incidents

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



External Links

The following links may be useful in providing additional information regarding online safety and are referred to on the school's website:

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
Childline: www.childline.org.uk
Childnet: www.childnet.com
Click Clever Click Safe Campaign: http://www.nidirect.gov.uk/click-clever-click-safe
DigitalParenting:
https://www.vodafone.co.uk/cs/groups/public/documents/webcontent/vfcon096227.pdf
Digizen: www.digizen.org.uk
Internet Watch Foundation (IWF): www.iwf.org.uk
Kidsmart: www.kidsmart.org.uk
Think U Know website: www.thinkuknow.co.uk
UK Safer Internet Centre: https://www.saferinternet.org.uk/
Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Appendix

Baxenden St John's CE Primary School

Staff, Governor and Visitor

Acceptable Use Agreement

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school eSafety coordinator.

- I will only use the school's email / Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware of software without permission of the E-safety coordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ..... Date .....

Full Name .....(printed)

KS1

ACCEPTABLE USE POLICY
for EYFS/KS1

How to stay safe when I use computers:

I will ask a teacher if I want to use the computers.

I will only use activities that a teacher has asked me to use.

I will take care of the computer and other equipment.

I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher if I see something that upsets or worries me.

I know that if I break the rules I might not be allowed to use a computer.

I have read and understood these rules and agree to follow them

Name of Pupil .....

Class .....

Signed .....

Date .....

Parents/Carer countersignature

As the parent/carer of the above pupil, I understand that the school has discussed the Acceptable Use Agreement with my son/daughter as part of a whole school commitment to online safety both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems , to ensure that young people will be safe when they use the internet and ICT systems.

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have any concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the Internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Name of Parent/Carer .....

Signed .....

Date .....

KS2

I agree to follow these rules when using any digital technology:

I will ask permission from a teacher before using ICT equipment and will use only my own login and password.

To protect myself and other pupils, if I see anything I am unhappy with or receive messages I do not like, I will immediately close the page and tell an adult.

I will not access other people's files or send pictures of anyone without their permission.

I will not bring CDs or memory sticks into school unless I have permission and they have been checked to ensure that they are virus free.

Where work is protected by copyright, I will not try to download copies (including music and videos)

I will not use my mobile phone in school for any reason. If I do bring my phone to school I will follow school rules and hand it in at the office on arrival.

I understand that the school may check my computer files and may monitor the internet sites I visit.

If I am involved in incidents of inappropriate behaviour that involve other members of the school community e.g. cyberbullying, using images/information without permission, the school will take action according to the Behaviour policy.

I understand that if I do not follow these rules I may not be allowed to use ICT in school and my parents/carers may be contacted.

I have read and understood these rules and agree to follow them

Name of Pupil .....

Class .....

Signed ..... **Date** .....

Parents/Carer countersignature

As the parent/carer of the above pupil, I understand that the school has discussed the Acceptable Use Agreement with my son/daughter as part of a whole school commitment to online safety both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have any concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the Internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Name of Parent .....

Signed ..... **Date** .....

Home / School Agreement

In order to create a safe environment for pupils and staff when taking part in Zoom live lessons, we would like you to discuss the following protocols with your child/ren:

By accepting the Zoom meeting ID and joining the meeting, with parental responsibility, you agree to the terms set out in this document.

1. Zoom is only to be accessed by a device in a communal family space.

2. An adult should ideally supervise it.

3. Attendees should be dressed appropriately.

4. The meeting ID is to remain confidential and not to be shared to anyone that it was not designated to.

5. Participants do not record, take photos or screenshots of the Zoom meeting.

6. Information or comments about the online lesson are not to be shared on social media, particularly any Baxenden class/parent WhatsApp groups – if this happens, the parents will be contacted by Mrs. Green.

7. If there are any concerns about the online lesson, these must be communicated to the head teacher only by the head teacher's email: head@baxenden.lancs.sch.uk

8. The Zoom lesson will be recorded by the hosting teacher and stored in line with the school GDPR and Online Safety policy.

9. For participants, the host teacher will disable some Zoom facilities. This includes but is not limited to the screen record function, chat and screen share.

10. Finally, the same behaviour expectations that are set within a classroom apply to the Zoom and fall within the remit of our normal Behaviour policy. The teachers reserve the right to remove children from meetings where behaviour does not follow our expectations.