

BILLINGHAY CHURCH OF ENGLAND PRIMARY SCHOOL
ONLINE SAFETY POLICY
March 2026

Introduction

This Online Safety Policy outlines the commitment of Billingham C of E Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school 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). Billingham C of E Primary 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.

This Online Safety Policy has been developed by the Online Safety Lead and Safeguarding Lead made up of: Mrs. Claire Pool and Mr. Richard Allen.

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, pupils and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – pupils, all staff, governing body, parents.

Safeguarding is a serious matter at Billingham Church of England Primary School and we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to our pupils or liability to the school.

This policy is available for anybody to read on our school website; upon review all members of staff will sign as read and understood the online safety policy. A copy of this policy and the Pupil Acceptable Use Policy will be sent home with pupils when they join the school and when the policy is amended with a permission slip. Upon return of the signed permission slip

and acceptance of the terms and conditions, pupils will be permitted access to school technology including the Internet.

Headteacher Name: Mr R Allen

Signed:

Chair of Governors: Mr S Atkinson

Signed:

Review Date: March 2026

Next Review: March 2027

1. Roles & 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, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Governing Body

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor)
- reporting to relevant *governors group/meeting*
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards.

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Headteacher

- 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 is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher 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 headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/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.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.

- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Designated Safety Lead (DSL)

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out.
- attend relevant governing body meetings/groups.
- report regularly to headteacher/senior leadership team.
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety).

Online Safety Lead

The Online Safety Lead will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL).
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments.
- have a leading role in establishing and reviewing the school online safety policies/documents.
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond.
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners.
- liaise with technical staff, pastoral staff and support staff (as relevant).

- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
 - content
 - contact
 - conduct
 - commerce

Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme.

This will be provided through:

- Purple Mash.
- PHSE and SRE programmes
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

IT Provider

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy 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 DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority 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 Mrs. Pool or Mr. Allen for investigation and action.
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- monitoring systems are implemented and regularly updated as agreed in school policies.

Teaching and support staff

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 use agreement (AUA).
- they follow all relevant guidance and legislation.
- all digital communications with learners, parents and carers and others should be on a professional level and only carried out using official school systems and devices (where staff use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements).
- they immediately report any suspected misuse or problem to Mrs. Pool or Mr. Allen for investigation/action, in line with the school safeguarding procedures.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- ensure 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 are 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 lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies.
- there is 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.
- they adhere to the school's technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity.
- they have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies.
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy.
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.

- 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.

Parents and carers

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website.
- providing them with a copy of the learners' acceptable use agreement.
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc.
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed).

2. Technology

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation, cyberbullying: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material;
- contact: being subjected to harmful online interaction with other users; and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

The use of Artificial Intelligence (AI) systems in School

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of

equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools..

- Staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- The school will audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- The school will support parents and carers in their understanding of the use of AI in the school.
- AI tools may be used to assist teachers in the assessment of learners' work, identification of areas for improvement and the provision of feedback.
- Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

Filters and monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

- checks on the filtering and monitoring system are carried out by the OSL or DSL using SWGfL Test Filtering termly.

Billinghay Church of England Primary School uses a range of devices including PC's, laptops and ipads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering

A member of the SLT and a governor, are responsible for ensuring these standards are met. Roles and responsibilities of staff and third parties, for example, in-house or third-party IT support are clearly defined.

- the school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL 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, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures.
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes.
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- There are regular checks of the effectiveness of the filtering systems . Checks using SWGfL Testfiltering.com are undertaken across a range of devices and the results recorded termly.
- Devices that are provided by the school have school-based filtering applied irrespective of their location.

Monitoring

The school has monitoring systems in place, agreed by senior leaders and technical staff, to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that monitoring is in place.
- There are effective protocols in place to report abuse/misuse. 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.
- The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review is conducted by members of the senior leadership team, the designated safeguarding lead, and technical staff. It will also involve the responsible governor. The results of the review will be recorded and reported as relevant.
- Devices that are provided by the school have school-based monitoring applied irrespective of their location.
- monitoring enables alerts to be matched to users and devices.
- where AI –supported monitoring is used, the purpose and scope of this is clearly communicated.

Email Filtering

We use software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Passwords

All staff and students will be unable to access any device without a unique username and password. Staff passwords will change on a termly basis or if there has been a compromise, whichever is sooner. Pupil passwords will be changed if there has been a compromise. IT Support will be responsible for ensuring that passwords are changed.

Anti-Virus

All capable devices will have anti-virus software ESET endpoint. This software will be updated at least weekly for new virus definitions. F1 Group will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

3. Safe Use

Internet

Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this Online Safety Policy and the staff Online Safety Policy; pupils upon signing and returning their acceptance of the Acceptable Use Policy.

Internet activity will be monitored to ensure, as much as possible, that users are not exposed to illegal or inappropriate websites, including terrorist and extremist material and to ensure,

as much as possible, that users do not actively seek access to illegal or inappropriate websites including terrorist and extremist material.

We must ensure that our pupils are safe from online terrorist and extremist material. This is typically by appropriate levels of filtering and monitoring.

What will happen in the event of a pupil being exposed to offensive or upsetting material?

If there is an incident in which a pupil is exposed to offensive or upsetting material, the school will wish to respond to the situation quickly by following these steps:

- all pupils will be taught to switch off the monitor and report what they have seen to the teacher in charge;
- support will be given to the pupil/pupils involved, the Headteacher will inform parents/carers and they will be given an explanation of the course of action the school has taken;
- the Online Safety Lead will be informed and report the URL (address) and content to our IT Support.
- Class teachers will give general guidance as a reminder of what to do in this event.

Email

All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Students are permitted to use the school email system, and as such will be given their own email address.

Management of Pupil Email

Pupils will learn how to use an e-mail application and be taught e-mail conventions. Staff and pupils will begin to use e-mail to communicate with others, to request information and to share information.

- Communications with persons and organisations will be managed to ensure appropriate educational use and the good name of the school is maintained.
- The forwarding of chain letters will be banned.
- Pupils may send e-mail as part of planned lessons using their e-mail addresses.
- E-mail sent out of school must be approved before sending.
- Pupils must not reveal details of themselves or others such as addresses or telephone numbers or arrange to meet anyone in e-mail communications.
- Pupils must ask an adult before they open an email so an adult can be present to read the received email.

Photos and videos

Digital media such as photos and videos are covered in the schools' Use of Photographs Policy. All parents must sign a parental consent slip when their child joins school or when the policy is amended; non-return of the permission slip will not be assumed as acceptance.

Social Networking

Billinghay Church of England Primary School is supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within our school and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the Online Safety Lead, who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school.
- Facebook – used by staff in school.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

Notice and take down policy

Should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Management of Publishing on the Web

The school web site is there to celebrate good work, promote the school and publish resources for projects or homework. As the school's web site can be accessed by anyone on the Internet, the security of the staff and pupils must be maintained.

- Class teachers are responsible for organising the information to be entered onto the web site.
- All material must be the author's own work, credit other work included and state clearly the author's identity or status.
- The point of contact on the web site will be the school's address and telephone number. Home information or individual e-mail identities will not be published.
- Group photographs should not have a name list attached and any child featuring in a photograph must have parental permission allowing them to be published on the site.

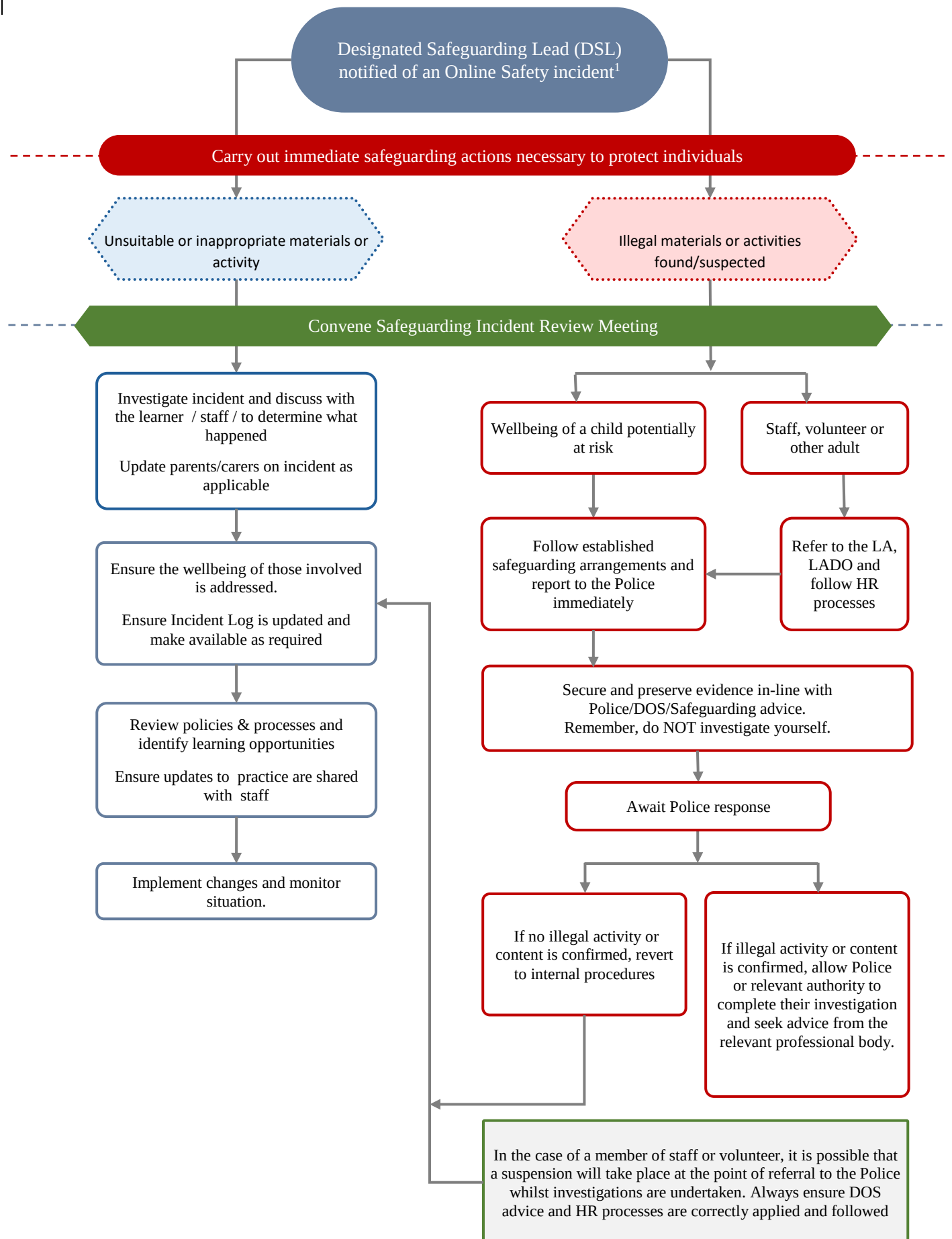
Reporting and responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made 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.
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff 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 the incident must be escalated through the agreed school safeguarding procedures, this may include:
 - Non-consensual images
 - Self-generated images
 - Terrorism/extremism
 - Hate crime/ Abuse
 - Fraud and extortion
 - Harassment/stalking
 - Child Sexual Abuse Material (CSAM)
 - Child Sexual Exploitation Grooming
 - Extreme Pornography
 - Sale of illegal materials/substances
 - Cyber or hacking offences under the Computer Misuse Act
 - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority.
- where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss.
- where there is no suspected illegal activity, devices may be checked using the following procedures:
 - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
 - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
 - ensure that the relevant staff 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.

- 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 (as relevant)
 - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident.
- incidents should be logged (See online safety log sheet in appendix)
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions.
- learning from the incident (or pattern of incidents) will be provided to:
 - staff, through regular briefings
 - learners, through assemblies/lessons
 - parents/carers, through newsletters, school social media, website
 - governors, through regular safeguarding updates
 - local authority/external agencies, as relevant

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.



Training and Curriculum

It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues.

Online Safety for pupils is embedded into the curriculum; whenever technology is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

Staff are given annual online safety training and parents are offered annual training through informative emails and videos covering a range of online safety issues.

Appendix 1

KS1 children

My name is _____

Learner Acceptable Use Agreement – for younger learners (Early Years/KS1)

Our Technology Rules

I will follow these rules to use computers, tablets and the internet safely at school.

Staying Safe

- My teacher will watch what I do on computers, tablets and the internet to keep me safe.
- I will keep my passwords secret and tell my teacher if I need help.
- I understand that people online are not always who they say they are. I will only talk to people online if my teacher or a trusted adult says it's OK.
- I will not share my name, address, or pictures without asking my teacher or a trusted adult first.
- If I see something that makes me feel worried or upset, I will tell my teacher or a trusted adult straight away.
- I will only use apps, games or websites my teacher says are safe.

Using Technology Kindly

- I will be kind when using technology, just like I am in real life.
- I will take care of the computers and tablets I use.
- I will only look at things my teacher says are OK.

Making Good Choices

- I will ask my teacher before I use someone else's pictures or work.
- I will take breaks from screens and do other fun things too.
- I know that I can say no / please stop to anyone online who makes me feel sad, uncomfortable, embarrassed or upset.
- I will ask for help from a trusted adult if I am not sure what to do or if I think I may have done something wrong.

What Happens If I Forget the Rules

- If I forget the rules, my teacher will help me learn to make better choices next time.

These rules help us all stay safe and have fun using computers and tablets at school!

Signed (parent):

Learner Acceptable Use Agreement – for KS2

Acceptable Use Agreement

I agree to use the school's digital systems safely and responsibly to protect me, other learners and the school.

Keeping Safe Online

- The school will check how I use devices and the internet to keep everyone safe.
- I will keep my usernames and passwords private and tell a trusted adult if someone else knows them.
- I will be careful when talking to people online and will only talk to people I know and trust.
- I will not share personal information like my name, address, or photos without asking a trusted adult.
- I will only take or share images of myself, or others, when fully dressed.
- If I see or hear something online that worries or upsets me, I will tell a trusted adult straight away.
- I will only meet people I have spoken to online if a trusted adult is with me.

Using Computers and the Internet Sensibly

- I will only use devices, apps and sites that I am allowed to, and will check if I am unsure.
- I will always ask permission and check with a trusted adult before using someone else's work or pictures.
- I will make sure the information I find online is true by checking carefully.
- I will only use apps or tools, like AI, that my teacher has said are OK, and I will ask for help if I'm unsure.
- I will not copy or use music, videos, or games unless I have permission.
- I will tell a trusted adult about any damage to devices or if anything else goes wrong.
- I will check with trusted adults before clicking on any unexpected messages or links (even if these look as though they are from people that I already know).

Being Respectful and Responsible

- I will treat others kindly online, just as I do in real life.
- I will make good choices about what I share online to protect myself and others.
- I will spend a healthy amount of time using devices and make time for other activities too.

- I will always think about how my behaviour online could affect me, my friends, and my school.

What Happens If I Break These Rules

- If I don't follow these rules, my teacher may stop me from using computers or devices, speak to my parents, or take other actions to help me make better choices in the future.

By following these rules, I can enjoy using technology safely and responsibly.

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

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: Group/Class:

Signed: Date:

.....

Appendix 2

BILLINGHAY CHURCH OF ENGLAND PRIMARY SCHOOL

Online Safety Incident Log

Details of incident			
Date		Time	
Where did the incident occur?			
Name of person reporting incident		Who was involved in incident (please tick)	Child: Staff Member: Other (please specify):
Names of those involved			
Type of incident (please tick)	Bullying/harassment: Online bullying or harassment (cyberbullying): Sexting (self taken indecent imagery): Deliberately bypassing security or access: Hacking or virus propagation: Racist, sexist, homophobic religious hate material, terrorist or extremist material: Other (please specify):		
Description of incident			
Nature of incident (please tick)	Deliberate access: Accidental access:		
Did the incident involve material being (please tick)	Created: Viewed: Printed: Shown to other: Transmitted to others: Distributed:		
Could this incident be considered as (please tick)	Harassment: Grooming: Cyberbullying: Sexting: Breach of AUP: Other (please specify):		
Action Taken			

Outcome of incident/investigation	
Learning from the case and recommendations	

Signed:

Print name:

Date: