St Aidan's
Church of England Primary Academy
A member of CTDARI

'Fulfilling potential and growing in God.'

Acceptance, Love, Wisdom, Accountability, Youthfulness, Service

Our Vision

At St. Aidan's, not only do we want our children to become happy and well rounded individuals; we aim to nurture and equip children to be resilient, enthusiastic and effective communicators and learners who are able to use their experiences and technology skills to achieve their fullest potential allowing them to excel in the careers of the future and grow in God.

'I came that they may have life and live it to the full' John 10.10

Online Safety Policy

Updated: November 2024

This policy will be reviewed at least annually, and following any concerns and/or updates to national/local guidance or procedures.

The DfE guidance "Keeping Children Safe in Education" states: "Online safety and the school or college's approach to it should be reflected in the child protection policy"

1. Aims

St Aidan's CE Primary Academy aims to:

- To draw together the range of statutory guidance and best practice
- is supplemented by a series of related acceptable use agreements used within the school as best practice, including that of staff, children and parents.
- Allocates responsibilities for the delivery of the policy
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- establishes clear procedures, in the form of a flow chart, to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, while tracking online safety incidents in a robust and timely manner
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- will be made available to staff at induction and through normal communication channels is published on the school website
- describes how the school will help prepare learners to be safe and responsible users of online technologies.

2. The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

1. Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
2. Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

3. Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
4. Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

3. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, the Online Safety Act, Keeping Children Safe in Education, and its advice for schools on:
Teaching online safety in schools, Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff, Relationships and sex education and Searching, screening and confiscation
It also refers to the DfE's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

4. Roles and responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While members of the school staff are responsible for the reporting of any safeguarding concerns, the following sections outline the online safety roles and responsibilities of individuals and groups within the school. Staff should be aware when reporting online safety concerns that in the log provided on My Concern, staff highlight the risk to the child/children involved.

4a. The local governing committee

The DfE guidance "Keeping Children Safe in Education" states:

"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"

"Governing bodies and proprietors should ensure an appropriate senior member of staff,

from the school or college leadership team, is appointed to the role of designated safeguarding lead."

Our governing board will discuss online safety, and monitor online safety logs (which will be recorded on my concern) as provided by the online safety lead, with DSL training. The link governor will oversee online safety.

4a. All governors will:

- Ensure that they have read and understand this policy before approving and reviewing its effectiveness.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (see ICT Acceptable use policy)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
- Be a part of regular meetings with the OSL and DSL's which share anonymised reports from My Concern.
- Ensure the filtering and monitoring systems are effective
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards.
- membership of the school 'Digital Leader' Group

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

4b. The headteacher and Senior Leadership Team

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.

4c. The Designated Online Safeguarding Lead

They (the DSL) "are able to understand the unique 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 at school or college"

They (the DSL) "can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

They (the DSL) have attended additional 'Online Safety Training' provided by Schools Safeguarding in order to support them within the role.

The DSL and Deputy DSL takes responsibility for online safety in school, in particular:

- Hold the lead responsibility for online safety, within their safeguarding role. At St Aidan's CE Primary school this lead is Mrs Hayley Hargreaves.
- 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
- Disseminate the above training in the form of further staff training on online safety.
- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy, ensuring they are logged on my concern and resolved in line with the school behaviour and safeguarding policy. (See flow chart in appendix)
- Liaising with other agencies and/or external services if necessary, including school staff and IT providers.
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Report regularly to headteacher/senior leadership team and the governing body.

4e. Online Safety Lead The Online Safety Lead will:

- lead the Digital leaders group with the support of the HT
- 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 (school/local authority/MAT/external provider) 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:

o content
o contact
o conduct
o commerce

4f. The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitor the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any incidents of cyber-bullying are reported to the DSL or deputy DSL's

4g. Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated Safeguarding whole school curriculum map which will identify where children are specifically taught how to safeguard themselves.
This will be provided through:

- A discrete programme PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Antibullying week.
- 'Be internet aware' additional curriculum offer in KS2.
- Junior Jam curriculum coverage as identified in their own progressive curriculum

4h. All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems (see ICT Acceptable use policy), and ensuring that pupils follow the school's terms on acceptable use (by signing the home school agreement)
- Working with the DSL's to ensure that any online safety incidents are logged (on my concern) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately and logged onto My Concern
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Staff have a responsibility to monitor children's internet use / screen during the school day.
- Staff are not to provide technology activities during indoor playtime or lunchtime as this can not be monitored safely.
- Staff should not assume that the filtering and monitoring systems alone are enough to safeguard children in the classroom, and should actively monitor at all times.
- Where necessary and searches need to be made in line with the national curriculum, staff should enter browsing content onto the school record log.

4i. 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 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.

4j. Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

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.
- Identifying the online safety lead across the school
- providing them with access to a copy of the learners' acceptable use agreement publish information about appropriate use of social media relating to posts concerning the school. Available on the school website and emailed out at the beginning of the academic year.
- 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)
- Ensure that your child/ren are not accessing inappropriate apps, (such as, but not limited to, whatsapp, tiktok, snapchat) on YOUR personal devices.
- Talk to your children about online safety and set clear rules about what apps they are allowed to use.
- Use parental control features to block inappropriate apps and websites.
- Monitor your children's online activity and be aware of what they are doing.
- Encourage your children to talk to you if they see anything upsetting or concerning online.

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (on the home school agreement via a google form)
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

4k. Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

4l. Filtering and Monitoring

Cidari have employed 'On247' as an external company to provide our filtering and monitoring services. The Online Safety Leader has met with the company and discussed the needs of the school improving the frequency of suspicious searches and the layout of the reports received.

The online safety lead will test the filtering and monitoring system, logging the date and time of these on the school calendar. These checks will be completed alongside our online safety governor, where appropriate.

5.Digital Leaders

Digital leaders will be voted by class members in Autumn term 2 (Autumn Term 1 from September 2025) They will meet every fortnight with the OSL. They will discuss concerns that the children are raising and spread key messages to the classes. They will plan assemblies for parents and online safety activities over the course of the academic year.

6. Educating pupils about online safety

When children access the chrome books a 'pop up' screen will appear reminding children of the measures they can take to protect themselves and keep themselves safe online.

Online safety will be discussed by the class teacher with the children every time the chrome books or online devices are used. The following screen will be displayed:

A whole school curriculum map has been produced identifying where children are taught how to keep themselves safe, including online safety. It is taken from the guidance on relationships education, relationships and sex education (RSE) and health education.
All schools have to teach: Relationships education and health education in primary schools. This whole school document takes into account the 'Be Internet Legends' curriculum to supplement the national curriculum. Alongside this a 'Safeguarding within the Curriculum' is being developed throughout this academic year, alongside curriculum leaders to ensure our children have the best possible education on how they can keep themselves safe in and out of school.

As a school we remain proactive and respond to the needs of the children and the concerns and issues which are highlighted to us via parents and children alike. As a result of this we will adapt the provision offer as and when we feel it is necessary.

The National Curriculum states the following:
In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in Computing and PSHE lessons.
If appropriate, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

7. Educating parents about online safety

- St Aidan's CE Primary Academy will raise parents' awareness of internet safety on Class Dojo, and information via our website

https://staidansblackburn.co.uk/parents/online-safety

- This policy will also be shared with parents. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the Deputy DSL.
- Parents will be invited into school by our Digital Leaders, for planned events to share their child's online learning. Opportunities will then be created for teachers to discuss with parents how children can keep themselves safe, online safety assemblies / celebrations / class dojo messages directly from children.
- School will provide an acceptable use agreements will be sent out to parents to complete and return to school.
- Online safety meetings will be held with parents, ideally once a term.
- Information will be shared on our weekly newsletter.

8. Cyber-bullying

8a. Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy)

8b. Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will use aspects of the curriculum to cover cyber-bullying. This includes during personal, social, health and economic (PSHE) education lessons.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (recorded on Every).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

8c. Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. Any devices that are brought into school are locked away and children do not have access to them throughout the school day.
When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or

- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.
Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

9. Cyber-attacks

St Aidans is a Google school and the IT manager is responsible for conducting a full security check. All staff have undertaken online training 'Cyber Security' at the request of the CEO of our MAT. St Aidan's follows the basic principles of good cyber security. These include powerful passwords, watching out for phishing, NO use of USB and pen drives and ensuring all devices have passcodes and software is kept up to date. Further guidance can be found on the 'Cyber Security Advisory Note' emailed out on 23rd September 2024. As part of the MAT's Cyber security protection system there will be a forced password reset across the academy.

All staff members will take appropriate steps to ensure their devices remain secure. At St Aidan's, we use Google drive to ensure documents remain in a safe online space. Steps that need to be taken include, but are not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

10. Online abuse and exploitation

Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it. The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the

school premises or using school-owned equipment. All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the DSL or Deputy DSL and dealt with in line with the Child Protection and Safeguarding Policy.

11. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (see ICT Acceptable use policy and home school agreement).
Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
The ICT Manager will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

12. Staff using work devices outside school

Staff members must not use the device in any way which would violate the school's terms of acceptable use. Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from the ICT Manager or DSL and Deputy DSL.

13. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, incidents are recorded on my concern and the safeguarding leads are notified. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate, with reference made the code of conduct.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the (ICT acceptable use policy). The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The academy trust and school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

14. Artificial Intelligence (AI) and Online Safety

As technology continues to evolve, AI is becoming increasingly integrated into our daily lives, including education. While AI offers many benefits, it's important to be aware of the potential risks and to use it responsibly.

Here are some ways St Aidans' aims to use AI / Gemini safely within the school and wider community:

- **Staff Training:** Ensure teachers are well-trained in using AI tools appropriately and ethically. This includes understanding the limitations and biases of AI. This training was held at our Cidari INSET in October 2024.
- **Parental Involvement:** The Online Safety Lead will communicate openly with parents about how AI is used in the classroom and address their concerns.
- **Critical Thinking:** Students and staff will be encouraged to think critically about the information generated by AI. As part of the online curriculum offer, they will be taught to verify information from multiple sources and to be aware of potential biases.
- **Digital Citizenship:** Integrate lessons on digital citizenship into the curriculum with British Values and our school values at the heart of all we do. This includes teaching students about online safety, responsible use of technology, and the ethical implications of AI.
- **Data Privacy and Security:** Adhere to strict data privacy and security protocols when using AI tools. Only collect and process the minimum amount of personal data necessary.
- **Regular Review:** Regularly review and update your AI policies and practices to stay up-to-date with the latest developments in AI and online safety.

By following these guidelines, you can create a safe and positive learning environment where AI is used responsibly and ethically.

15. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). Staff are also directed to our online safety page on our school website.

All staff have undertaken the 'Cyber Safety' course provided on 'me learning' at the request of the MAT CEO.

By way of this training, all staff will be made aware that:
Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content

Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our safeguarding and child protection policy.

16. Monitoring arrangements

All staff log behaviour and safeguarding issues related to online safety onto my concern. This is then monitored by the DSL and deputy DSL. This policy will be reviewed every year by the online safety leader. At every review, the policy will be shared with the governing board.

16a. Policy development, monitoring and review

This Online Safety Policy has been developed by the Online Safety Group made up of:
Designated safeguarding lead (DSL)
Online Safety Lead (OSL) staff – including teachers/support staff/technical staff Governors
Parents and carers

16b. Schedule for development, reporting and review

The Online Safety Policy was approved by the school governing body.	
The implementation of this Online Safety Policy will be monitored by;	Kelly Harrison (Head Teacher) Hayley Hargreaves (Deputy Head and Online Safeguarding Lead)
Monitoring will take place at regular intervals;	Anually
The governing body will receive a report on the implementation of the Online Safety Policy (including anonymous details of online safeguarding incidents at regular intervals)	Once a term
The Online Safety Policy will be reviewed annually, or when any significant new technological developments, new threats or updates to statutory guidance are announced. The next anticipated review date will be:	September 2025
Should serious safeguarding incidents take place, the following external personnel / agencies should be informed (including but not limited too);	Schools Safeguarding team, police, MASH etc.

16c. Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:
logs of reported incidents and the nature of these incidents.
Filtering and monitoring logs
internal monitoring data for network activity
surveys/questionnaires of: learners / parents and carers / staff.

H Hargreaves

ONLINE SAFETY LEAD

November 2024