St. Alban & St Stephen
Catholic Primary School and Nursery

‘Learning and growing with God by our side.’

Online Safety Policy

Approved by:	Full Governing Body	**Date:** January 2025
Next review due by:	January 2026	

1. Aims

At St Alban & St Stephen Catholic Primary School & Nursery, we aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **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
- **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
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, 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
- 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.

3. Roles and responsibilities

3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The governing body will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

Ensure they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures

Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is 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

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead (DSL)/ Headteacher

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL/ headteacher takes lead responsibility for online safety in school, in particular:

Ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

Ensuring the governing body review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.

Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.

Ensuring that weekly checks on the filtering and monitoring systems are made and recorded by a designated member of the Office staff.

Working with the ICT support to make sure the appropriate systems and processes are in place.

Working with the ICT support 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's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

3.4 The ICT Support

The ICT support (Platinum IT) is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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 monitoring the school's ICT systems on a weekly basis (run by the school office)
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are reported to the headteacher who will dealt with these incidents appropriately in line with this policy using appendix 3
- Ensuring that any incidents of cyber-bullying communicated to the headteacher who will deal with these appropriately in line with the school behaviour policy

See Appendix 4 for further detail. This list is not intended to be exhaustive.

3.5 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 and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting these incidents to the DSL/ headteacher
- Following the correct procedures by speaking to the DS/ headteacher if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL and deputies to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- 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'

3.6 Parents/carers

Parents/carers 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 (appendix 1)

Parents/carers 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

Parent resource sheet – Childnet

3.7 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. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

Relationships education and health education in primary schools

Primary schools:

In **Key Stage (KS) 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 (KS) 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 other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher/ DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 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 discuss cyber-bullying with their class.

Teachings will also cover cyber-bullying in other aspects of the curriculum. This includes personal, social, and health (PSHE) education, and other subjects where appropriate including Relationships, Health and Sex Education.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

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/headteacher will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can confiscate any electronic device that they have reasonable grounds for suspecting:

Poses a risk to staff or pupils, and/or

Is identified by the school as a banned item, and/or

Is evidence in relation to an offence

If an electronic device belonging to a child is confiscated, the head teacher will call the child's parent or carer to come into school to collect the item in person and will explain why it has been confiscated.

However, if there is reason to suspect that the electronic device could be evidence in relation to an offence, the police will be called and any advice given by the police with regard to the electronic device will be followed.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

Not view the image

Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

St. Alban & St Stephen Catholic Primary School and Nursery recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

St. Alban & St Stephen Catholic Primary School and Nursery will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils in Year 6 who walk to or from school by themselves may bring mobile devices into school, but they must hand them into the office at the beginning of the day and collect them at the end of the day. They should not be used on school premises. Before bringing a mobile device in, parents/ carers must sign a permission form to say that their child will walk to or from school by themselves and is allowed to bring a mobile phone to school. Pupils in Year 5 may only bring a 'non-smartphone' which does not have access to the internet. From September 2026, no pupil will be allowed to bring a smartphone to school as part of our 'Smartphone-free School' initiative. No pupil below Year 5 is allowed to bring electronic devices of any kind in to school.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is 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

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 2.

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 our ICT provider.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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 staff disciplinary procedures / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. 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).

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, threatening, 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 up the risks
- 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 deputies 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 child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by a member of the senior leadership team. At every review, the policy will be shared with the governing body. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1:

St Alban & St Stephen Catholic Primary School & Nursery

Online Safety Acceptable Use Agreement for Pupils & Parents

‘Learning and growing with God by our side.’

My online safety rules - Pupils

- I will only use school IT equipment for activities agreed by school staff.

- I will not use my personal email address or other personal accounts in school when doing school work.

- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.

- I will only open email attachments if it has been approved by a member of school staff in school or a parent/carer out of school.

- In school I will only open or delete my files when told by a member of staff.

- I will not tell anyone other than my parents/carers my passwords. I will not use other people’s usernames or passwords to pretend to be them online.

- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.

- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.

- If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or my parent/carer immediately.

- I will not give out my own or other people’s personal information, including: name, phone number, home address, interests, schools or clubs. I will tell my teacher or parent/carer if anyone asks me online for personal information.

- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent’s/carer’s permission.

- Even if I have permission, I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.

- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.

- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.

- I understand that electronic devices are not allowed in school, including smartwatches, and I will follow the rules.

- I understand that only Year 5 and 6 pupils with signed permission from their parents can bring their mobile phones to school. If I am in Year 5 or 6 and I have signed permission from my parents, I understand that I must switch my mobile phone off and hand it in to my teacher as soon as I come into school. I understand that I am not allowed to use my mobile phone anywhere on school grounds.

- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.

- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may need to take action.

Appendix 2:

St Alban & St Stephen Catholic Primary School & Nursery

Online Safety Acceptable Use Agreement for Staff* and Governors

***including student teachers who are members of staff and volunteers if appropriate**

'Learning and growing with God by our side.'

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the Head teacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

- I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

Online conduct

- I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).
- I will report any accidental access to or receipt of inappropriate materials or filtering breach to the headteacher.
- I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.
- I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Social networking

- I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils even ex pupils up to the age of 25 years.
- When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.
- I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

- I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member. Supply staff will be given a login in that will only allow them very basic rights to the system.

Data protection

I will follow requirements for data protection as outlined in GDPR policy. These include:

- Photographs must be kept securely and 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 headteacher or governing body
- Personal or sensitive data taken off site must be encrypted

Images and videos

- I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.
- I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of email

- I will use my school email address or governor hub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email addresses or governor hub for personal matters or non-school business.

Use of personal devices

- I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.
- I will only use approved personal devices in designated areas and never in front of pupils.
- I will not access secure school information from personal devices (see policy).

Additional hardware/software

- I will not install any hardware or software on school equipment without permission of the IT Technician and the Headteacher.

Promoting online safety

- I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.
- I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to the DSL or the Deputy .

Classroom management of internet access

- I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.
- If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the children.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor.

(DIGITAL SIGNATURE OR SIGNATURE BELOW IS REQUIRED FROM ALL STAFF)

Signature …….…………………….………… Date ……………………

Full Name ………………………………….. (printed)

Job title ………………………………………………………………….

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3:

St Alban & St Stephen Catholic Primary School & Nursery

‘Learning and growing with God by our side.’

Online Safety Incident Reporting Form

Any member of the school community can raise a concern about an online safety incident. If you have witnessed or experienced an incident please complete the form below to help us to address the issue. It is important that you provide as much detail as possible. Once completed please hand this report to a member of the Senior Leadership Team.

Name of person reporting incident:				
Signature:				
Date you are completing this form:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young people	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else’s account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyber bullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	

Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else’s name to bring them into disrepute		Breaching copyright regulations	
Other breach of acceptable use agreement, please specify			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence available but do not attach.

Thank you for completing and submitting this form.

Appendix 4:

St Alban & St Stephen Catholic Primary School & Nursery

‘Learning and growing with God by our side.’

IT Safeguarding & Security Information

Antivirus\Malware – ESET Protect Cloud

The school utilises ESET Protect Advanced Cloud across all school servers\workstations which includes the following features:

- Cloud based console
- Modern Endpoint Protection
- File Server Security
- Full Disk Encryption
- Advanced Threat defence

More in depth information can be found here: https://www.eset.com/uk/business/protect-platform/

Web Filtering - RM SafetyNet

The school filtering is provided by RM SafetyNet.

Filtering Policies

The school currently uses WF1 filtering policy for staff and WF4 filtering policy for students, below is the list of available policies and their restrictions:

- WF1 is the least restrictive and can therefore be regarded as our baseline policy, being geared towards trusted users such as staff. It denies access to pornography, the promotion of illegal activities and to the propagation of hatred but most other material is allowed.
- WF2 is very similar to WF3. The main difference being that games websites are accessible. After school clubs for example, may wish to deploy this policy.
- WF3 is ideally suited for primary school children. YouTube and social networking sites such as Facebook are blocked. Restrictions are in place, denying access to non-educational games websites.
- WF4 is generally the same as WF3 but it restricts access to Twitter. Twitter is available on every other filtering policy

SSL Inspection

All school owned devices have the RM SafetyNet SSL certificate installed to them. This enables the filtering system to intercept\decrypt all HTTPS traffic to allow the filtering to apply the necessary safety features. Hfl Broadband operates a ‘whitelist’ which prevents certain websites being decrypted such as online banking websites.

Monitoring

The schools RM SafetyNet account can run filtering reports which provide the school with the ability to identify which IP address have been attempting to access inappropriate content online.

Alerting

There are three types of alerts available:

- Access (or attempts) to child sexual abuse content ('IWF Alerts')
- Extremist content ('Prevent Alerts')
- Custom alerts

If anything gets triggered, RM will contact HfL, who in turn will contact the school.

More in depth information about RM SafetyNet can be found here: https://www.rm.com/products/rm-safetynet

Servers and Workstation Updates

Server Monitoring\Updates – NinjaOne

Platinum IT monitors the school's server 24/7 with NinjaOne remote monitoring solution. This solution provides the following:

- Automated Patch Management – This keeps Windows updates up to date on the servers and any third-party software patched.
- Endpoint Monitoring – with access logs and device health and sends alerts to Platinum IT if any issues are found.

Workstation Updates – WSUS

Windows\Microsoft workstation updates are managed via WSUS (Windows Server Update Service), each site pulls down the updates to their local WSUS server which are then authorised and deployed to applicable workstations on an automatic schedule which is configured.

Backups – Onsite and Offsite

Onsite backups

Backup Server on each site is configured with Veeam Backup which then backs up to a NAS (network attached storage) device which is located away from the main server location. Infant site this device is in the Network Cab in the EYFS building and the Junior Site this currently is in the headteachers office but will be relocated to the Library Cabinet to increase the distance away from the servers. This backup is scheduled to take place nightly.

Offsite Backups

The school is currently using Veeam Replication to an offsite repository which is provided by a third-party company. This backup runs on the same schedule as the onsite backup. This solution is coming to its contract end, and we are looking at alternate providers to reduce costs.