St. Andrew's School

Online Safety Policy

Maintenance

Policy Written By	**James Pitcher**
Date of Policy	**01/09/2026**
Next Review	**01/09/2028**

Approved by The Director of Schools, Deborah Leek-Bailey – 01/09/2026

Online Safety Policy

This policy is applicable to all pupils, including those in the EYFS

1. Aims

St. Andrew's aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and visitors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: 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**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying,
- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

2. Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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.

3. Roles and Responsibilities

3.1 Education Development Trust

Education Development Trust has overall responsibility for monitoring this policy and holding the Principal to account for its implementation. The Trust will ensure that the systems used for

monitoring and filtering are robust, that pupils are taught about keeping themselves safe online, including building resilience to radicalisation (at an age-appropriate level), and that staff are trained in online issues.

3.2 The Principal

The Principal 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

Details of the School's Designated Safeguarding Lead (DSL) are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, by:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school (with support from the Computing Lead)
- Working with the Principal, ICT Manager, Computing Lead and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) 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 Anti-Cyber Bullying Policy or the child-on-child abuse guidance within the school Safeguarding Policy
- Ensuring the Computing Lead updates and delivers staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing reports on online safety in school to the Principal and Education Development Trust as appropriate

This list is not intended to be exhaustive.

3.4 The ICT Manager

The ICT Manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) 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 Anti-Cyber Bullying Policy or the child-on-child abuse guidance within the school Safeguarding Policy

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
- Understanding their roles and responsibilities, through training and guidance, for filtering and monitoring internet usage at school, and ensuring that content is suitable within their classes
- 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)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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 Anti-Cyber Bullying Policy or the child-on-child abuse guidance within the school Safeguarding Policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Principal 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 can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

  Digital Wellbeing, Childnet International: https://www.childnet.com/blog/digital-wellbeing-guidance-for-parents

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 are 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.

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

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Pupils will be encouraged to build resilience to any encounters with radicalisation (at an age-appropriate level).

5. Educating Parents about Online Safety

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

Online safety will also be covered during an annual Parent Workshop.

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

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

6. Social Networking

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day.

The school also strongly discourages children from using age inappropriate social networking outside of school. Should the staff be made aware of incidents or activities on these social networks, which has a direct effect on the children's behaviour or attitudes within school, then the school reserves the right to take action regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

7. Cyber-bullying

7.1 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Anti-Bullying Policy.)

7.2 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 form group, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff 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).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Anti-Cyber Bullying Policy or the child-on-child abuse guidance with the school Safeguarding 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 school will adopt a zero tolerance approach to any cyber bullying issues and all staff will challenge any abusive behaviour between pupils that come to their notice and will report on to the DSL immediately any issues of this nature. Please see Safeguarding Policy for further details about dealing with child-on-child abuse.

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.

7.3 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.

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

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

8. Acceptable Use of the Internet in School

All pupils, parents, staff and volunteers 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 and visitors (where relevant) to ensure they comply with the above.

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

9. Pupils using Mobile Devices in School

Pupils may bring mobile devices into school, but are not permitted to use them during school hours. They must be handed in to the school office at the start of the school day and then collected at the end of the day.

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.

Pupils do not have any access to 3G/4G/5G as all personal devices are handed in to the school office and phones are not allowed on school trips.

10. Staff using Work Devices Outside School

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

11. 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 the 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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

12. 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).

The 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.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed yearly by the Computing Leader.

14. Links with other policies

This Online Safety Policy is linked to our:

- Safeguarding Policy
- Behaviour and Discipline Policy
- Staff Disciplinary Procedures
- Concern and Complaints Procedure
- Anti-Cyber Bullying Policy

Mr. J. Pitcher
Computing Lead
St. Andrew's School

Policy Date: 1st September 2026

Policy Review Date: September 2027

Appendix 1: Acceptable Use Agreement (Pupils and Parents/Carers)

Information and Communications Technology
Acceptable-use Policy

Pupil guidelines for Internet-use

General

Pupils are responsible for good behaviour on the Internet, just as they are in a classroom or a school corridor. General school rules apply.

The Internet, primarily, is provided for pupils to conduct research, access information / apps appropriate for their work and back-up their work. Parent's/carer's permission is required before a pupil is granted access. Access is a privilege not a right and that access requires responsibility.

Individual users of the Internet are responsible for their behaviour and communications over the network. Users must comply with school standards and honour the agreements they have signed.

Computer storage areas (including any external storage media you bring to school) will be treated as school files and exercise books. Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or storage media are always private.

During school, teachers will guide pupils towards appropriate materials. Outside of school, families bear responsibility for such guidance as they must also exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

The following are not permitted within the school environment:

1. Sending or displaying offensive messages or pictures.
2. Using obscene language.
3. Harassing, insulting or attacking others.
4. Damaging computers, computer systems or computer networks.
5. Violating copyright laws.
6. Using others' passwords or accounts.
7. 'Hacking' into others' folders, work or files for any reason.
8. Intentionally wasting limited resources, including printer ink and paper.
9. Use of Social Media sites such as Facebook.

Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on internet/computer use.
2. Your parents/carers will be informed.
3. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
4. When applicable, police or local authorities may be involved.
5. If necessary, external agencies such as Social Networking or Email Member sites may be contacted and informed.

Pupils

- You must have your parent's/carer's permission before using the Internet.
- You must have a supervising teacher or member of staff with you at all times when using the Internet.
- Do not disclose any password or login name to anyone, other than the persons responsible for running and maintaining the system.
- Do not upload/send personal addresses, telephone/fax numbers or photographs of anyone (staff or pupils) at the school.
- Do not download, use or upload any material, which is copyright. Always seek permission from the owner before using any material from the internet. If in doubt do not use the material.
- Under no circumstances should you view, upload or download any material, which is likely to be unsuitable for children. This applies to any material of a violent, dangerous or inappropriate context. If you are unsure ask the supervisor.
- Always respect the privacy of files of other users.
- Be polite and appreciate that other users might have different views than your own. The use of strong language, swearing or aggressive behaviour is not allowed. Do not state anything, which could be interpreted as libel.
- Ensure that you have followed the correct procedures for using the Internet.
- Report any incident which breaches these rules to the Computing Teacher, your Form teacher or the Principal

I have read through the policy with my parent/ guardian and agree to abide by the rules stated in the I.C.T. Acceptable Use Policy. I understand the consequences if I do not.

Pupil Name: …… Form: ……..

Signed: …… Date: ……

Parent/Guardian Signature: …… Date: ……

Appendix 2: Acceptable Use Agreement (Staff, Volunteers and Visitors)

Information and Communications Technology
Acceptable-Use Policy

Whilst St. Andrew's encourages the creative use of Internet, Digital and Mobile Technology for learning, we recognise that all members of staff are responsible for the safeguarding of pupils and the appropriate use of ICT resources both internally and externally.

This policy must be read in conjunction with St. Andrew's Safeguarding Policy and Staff Code of Conduct.

Computer Equipment

Computers, laptops, tablets and other networked resources are available to staff in the school. These resources are intended for administrative and educational purposes, and may only be used for legal activities consistent with the rules and policies of the school.

All staff must take appropriate security measures to protect laptops, tablets, and any peripheral devices (for example digital cameras).

It is expected that staff will use computers as appropriate within the curriculum and that they will provide guidance and instruction to pupils in the use of the online curriculum. The computers, laptops and tablets are provided and maintained for the benefit of all staff. If a member of staff requires a laptop outside of school they must seek permission before doing so. When offsite, staff must continue to follow the guidelines outlined in this policy.

Email and Messaging

The school e-mail account will be the principal point of contact for all electronic communication and should be used for all correspondence involving school business.

Whilst our ICT support services provide filtering and virus protection staff should not:

- Use strong language, swearing or aggressive behaviour
- Open attachments to emails unless they come from someone you already know and trust. (They could contain viruses or other programs that would destroy all the information and software on your computer)
- Send or receive emails (or other forms of digital messaging) containing material that is likely to be unsuitable for children (This applies to any material of violent, dangerous, racist, or inappropriate content). If staff have any concerns over correspondence they receive electronically they should **not** delete the message and report the incident to a member of the SLT immediately.

Social Networks

St. Andrew's understands that you may use the internet, email and other types of electronic communication (including instant messaging and social networks like Facebook and Twitter) in your personal lives. However, many sites such as social networks have public visibility and staff must not post any content that may compromise the school safeguarding policy, staff code of conduct or post anything that may bring St. Andrew's or Education Development Trust into disrepute. The School owned IPods can be used to post appropriate news to the School Twitter and Facebook pages.

Computer Equipment

Permission must be sought before taking any IT devices off site. When using IT devices outside of school the acceptable usage policy still applies.

Teachers must not –

- Install or attempt to install, device drivers and software on the laptops without permission from the network administrator.
- Change settings on computers or laptops unless authorised by the Computing Co-ordinator, this includes Internet settings, browsers and system preferences

If using a laptop in or out of school you are continuously responsible for it. Any damage must be reported to the Computing Leader immediately.

You must not allow any external agency or support service to tamper with St. Andrew's hardware or software. Appropriate and safe care and storage of St. Andrew's laptops is expected at home.

Definitions of Unacceptable Usage

Unacceptable use of St. Andrew's computers and network resources may be summarised as, but not restricted to:

- Actions which cause physical damage to any ICT hardware, including peripherals (e.g. mouse, cables, wiring)
- Creating, displaying or transmitting material that is fraudulent or otherwise unlawful, likely to cause offence or inappropriate
- Threatening, bullying, intimidating or harassing staff, students or others
- Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights
- Defamation
- Unsolicited advertising, often referred to as "spamming"
- Sending emails that purport to come from an individual other than the person actually sending a message using, e.g. a forged address
- Attempts to use the ICT facilities for the purposes of bribery
- Attempts to break into or damage computer systems or data held thereon
- Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software, e.g. use of equipment which is inadequately protected against viruses and spyware
- Attempts to access or actions intended to facilitate access to computers for which the individual is not authorised
- Using the school network for unauthenticated access
- Using the ICT facilities for gambling
- Using the ICT facilities for carrying out any illegal trading activity
- Any other conduct which may discredit or harm the school, its staff or the ICT Facilities

Privacy and Monitoring

Passwords

Staff are reminded that the user is responsible and accountable for all activities carried out under their username. It is each member of staff's responsibility to keep their own and the school's data secure. Teachers are asked to log off or lock their pc, laptop or device when they are not at the machine, this includes short periods of time or when accessing the school's drives remotely. At the end of the day it is important staff 'shut down' their classroom computer and turn off the overhead projector so updates and backups can run.

Staff **must not**

- Share their passwords with anyone else (this is excepting shared accounts such as some of the Administrative accounts where it is recognised that passwords may need to be shared).
- Have their passwords on display or store their password where it may be found by others.

The school reserves the right for appropriately authorised staff to examine any data including personal data held on school systems.

It is also occasionally necessary to intercept network traffic. In such circumstances appropriately authorised persons will take all reasonable steps to ensure the privacy of service users. Logs will be kept of usage of ICT equipment; this will include dates and times when accounts were accessed.

Once a staff member has left the school the school holds the right to refuse access to emails and data stored on its network.

Printing

Whilst St. Andrew's realises that printing is necessary we encourage all staff and pupils to print responsibly. Printing should not be for personal use. St. Andrew's monitors printing and the SLT hold the right to change print quotas at any time.

When teaching in the ICT room, staff need to monitor and check the screen before giving pupils permission to print, especially in colour. **THINK BEFORE YOU PRINT!**

Laptops

Pupil Laptops

Networked laptops are available to borrow for use in the classrooms. The teaching staff member is ultimately responsible for the collection, transportation and safe return of each laptop to and from the laptop trolley. Any faults must be immediately reported to the Computing Leader.

Principles – BE PROFESSIONAL, RESPONSIBLE AND RESPECTFUL

- You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the school and your personal interests.
- You must not engage in activities involving social media, which might bring St. Andrew's into disrepute.
- You must not represent your personal views as those of St. Andrew's on any social medium.
- You must not discuss personal information about pupils, and other professionals you interact with as part of your job on social media.
- You must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations or St. Andrew's.
- You must be accurate, fair and transparent when creating or altering online sources of information on behalf of St. Andrew's.
- You must decline 'friend requests' from pupils if you receive any on your personal social media accounts.
- You must not discuss any personal information about pupils and their family members and colleagues, or any personal web space.
- Caution is advised when inviting work colleagues to be 'friends' on personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships.
- Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking, so that any other contact details are not given away.

Appendix 3: Anti-Cyber Bullying Policy

This policy is applicable to all pupils, including those in the EYFS

This policy applies to all pupils, including those in the Early Years Foundation Stage (EYFS). It should be read in conjunction with the School's Safeguarding and Child Protection Policy, Anti-Bullying Policy, Online Safety Policy, Behaviour Policy and ICT Acceptable Use Policy.

Aims

The aim of this policy is to ensure that all members of the school community understand how to prevent, identify and respond to cyber bullying. The school is committed to creating a safe, respectful, and secure digital environment in which pupils can learn without fear of harm.

We aim to:

- Prevent cyber bullying through education and safe systems
- Respond promptly and effectively to incidents
- Support victims and challenge perpetrators
- Work in partnership with parents and external agencies where appropriate

Definition of Cyber Bullying

Cyber bullying is the use of digital technologies to deliberately and repeatedly (or in some cases, via a single serious incident) harm, intimidate, or upset another individual.

This includes sending, sharing, or posting:

- Harmful, threatening, or abusive messages
- Embarrassing or humiliating images or videos
- False or defamatory content
- Content designed to exclude, harass, or intimidate

Cyber bullying can take place via mobile phones, computers, tablets, gaming platforms, and all forms of online communication.

School Approach

St. Andrew's School adopts a **zero-tolerance approach** to cyber bullying.

The school will:

- Treat all allegations seriously and respond promptly
- Ensure safeguarding procedures are followed at all times
- Support victims and manage perpetrators fairly and consistently
- Record and monitor all incidents
- Involve external agencies where appropriate, including the police or children's social care where there is risk of harm

All concerns must be reported immediately to the **Designated Safeguarding Lead (DSL)**.

Types of Cyber Bullying
Cyber bullying may include:

- Messaging-Based Bullying
  - Abusive or threatening text messages
  - Silent or nuisance phone calls
  - Misuse of messaging platforms or impersonation
- Image and Video-Based Bullying
  - Sharing humiliating or manipulated images
  - "Happy slapping" (recording and sharing physical harm)
  - Distribution of private images without consent
- Email and Account Misuse
  - Threatening or abusive emails
  - Fake accounts created to impersonate or defame others
- Social Media and Online Platforms
  - Bullying via platforms such as social networking sites, blogs, forums, or video-sharing services
  - Posting harmful comments, rumours, or exclusionary content
- Gaming and Live Chat Platforms
  - Harassment during online gaming
  - Abuse via chat rooms or instant messaging services

Mobile Phones and Personal Devices

- Pupils must not use mobile phones during the school day.
- Devices must be handed in at the start of the school day and collected at the end.
- Any misuse will be treated as a safeguarding and behaviour concern.

Staff must:

- Store mobile phones securely during working hours
- Not use personal devices to photograph or record pupils
- Use only school-approved devices for any pupil-related recording

Parents:

- May photograph school events but must not share images of other children online without consent.

Online Safety: Filtering and Monitoring

The school operates robust filtering and monitoring systems to safeguard pupils online.

The school will:

- Block access to inappropriate or harmful content
- Monitor internet usage in line with safeguarding expectations
- Maintain secure ICT systems protected against malware and unauthorised access
- Record and respond to online safety incidents appropriately

All monitoring systems are regularly reviewed and updated.

Staff Training

All staff receive:

- Safeguarding and online safety training at induction
- Annual refresher training on cyber bullying and online risks
- Regular updates via staff briefings and safeguarding communications

Staff are expected to:

- Recognise signs of cyber bullying
- Act promptly and report concerns to the DSL
- Follow safeguarding procedures at all times

Prevention and Education

The school actively educates pupils about online safety through:

- PSHE curriculum
- Computing lessons
- Assemblies and themed weeks (e.g. Online Safety Week)
- External workshops and parent sessions

Pupils are taught to:

- Use technology safely and responsibly
- Report concerns immediately
- Understand the consequences of online behaviour

Reporting and Response Procedures

Any member of the school community may report cyber bullying.

When an incident is reported:

1. Report immediately to the DSL or Principal
2. An initial safeguarding assessment is carried out
3. Evidence may be collected (screenshots, messages, logs)
4. Parents are informed where appropriate
5. Pupils are interviewed sensitively (victim, witnesses, alleged perpetrator)
6. Appropriate sanctions are applied in line with the Behaviour Policy
7. Support is provided for both victim and perpetrator
8. The incident is recorded on the school safeguarding/incident system
9. Monitoring continues to ensure no recurrence

Where appropriate, external agencies may be involved, including:

- Police (criminal activity)
- Children's Social Care
- Early Help services

Outcomes and Support

The school aims to ensure that:

- The victim feels safe and supported
- The behaviour stops immediately
- The perpetrator understands the impact of their actions
- Underlying causes are addressed
- Appropriate support and intervention are provided
- Behaviour improves over time

Parental Involvement

Parents are expected to:

- Report concerns promptly
- Avoid confronting other pupils or families directly
- Support the school in managing incidents
- Attend meetings where required

The school will:

- Communicate outcomes clearly
- Work in partnership with families
- Provide guidance and support resources

Guidance for Parents

Parents are encouraged to:

- Supervise children's online activity
- Use parental controls where appropriate
- Monitor apps, games, and social media use
- Encourage open communication about online experiences
- Seek advice from school if concerned.

Guidance for Pupils

Pupils are taught to:

- Tell a trusted adult immediately
- Not respond to abusive messages
- Save evidence where safe to do so
- Block and report harmful users
- Remember that bullying is never their fault

Sanctions

Sanctions may include:

- Loss of privileges
- Removal from activities
- Behaviour monitoring plans
- Internal exclusion

- Fixed-term or permanent exclusion in serious cases

All sanctions are proportionate, fair, and applied in line with the Behaviour Policy.

Review

This policy will be reviewed annually or sooner if required due to legislation, safeguarding updates or school need.

Key Statutory Guidance

This policy aligns with:

- Keeping Children Safe in Education (KCSIE)
- DfE: Preventing and Tackling Bullying (2017)
- DfE Cyberbullying Guidance (2014)
- Working Together to Safeguard Children

This policy should be read in conjunction with the School's Behaviour and Discipline Policy, Computing Policy, Online Safety Policy, ICT Acceptable Use Policy, Data Protection Policy and Anti-Bullying Policy. The Policy takes account of the following documents:

- DFE Cyberbullying: Advice for Headteachers and School Staff 2014
- DFE School Support for Children and Young People who are being Bullied 2014
- DFE Preventing and Tackling Bullying 2017
- DFE Advice for Parents and Carers on Cyberbullying 2014

Mrs F. Lakanu

Assistant Principal

St. Andrew's School

Policy Date: 1st September 2026

Review Date: September 2027

Appendix 1

Advice for Parents

- Don't wait for something to happen before you act. Make sure your child understands how to use these technologies safely and knows about the risks and consequences of misusing them.
- Make sure they know what to do if they or someone they know are being cyber bullied.
- Encourage your child to talk to you if they have any problems with cyber bullying. If they do have a problem, contact the school, the mobile network or the Internet Service Provider (ISP) to do something about it.
- Parental control software can limit who your child sends emails to and who he or she receives them from. It can also block access to some chat rooms.

- Moderated chat rooms are supervised by trained adults. Your ISP will tell you whether they provide moderated chat services.
- Make it your business to know what your child is doing online and who your child's online friends are. It is important that parents and carers ensure that their children are engaged in safe and responsible online behaviour.
- It is important that legal age advice is followed before allowing your child access to online platforms.
- Seek advice from school if you are unsure as to where to access the most appropriate and current information.

Suggestions for parents to stay involved

- Keep the computer or other electronic devices in a public place in the house. Periodically check on what your child is doing.
- Discuss the kinds of Internet activities your child enjoys.
- Be up front with your child that you will periodically investigate the files on the computer, the browser history files, and your child's public online activities.
- Search for your child's name online, look at his or her profiles and postings on teen community sites, review web pages or blogs.
- Tell your child that you may review his or her private communication activities if you have reason to believe you will find unsafe or irresponsible behaviour.
- Watch out for secretive behaviour as you approach your child when they are online, such as rapidly switching screens, changing passwords and for attempts to hide online behaviour, such as an empty history file.

Appendix 2

Advice for Pupils

- If you are being bullied, remember bullying is never your fault. It can be stopped and it can usually be traced.
- Don't ignore the bullying. Tell someone you trust, such as a teacher or parent, or call an advice line.
- Try to keep calm. If you are frightened, try to show it as little as possible. Don't get angry, it will only make the person bullying you more likely to continue.
- Look at the St. Andrew's Anti Bullying Policy online.

There is plenty of online advice on how to react to cyber bullying.

Text/Video Messaging

- You can turn off incoming messages for a couple of days.
- If bullying persists you can change your phone number (ask your Mobile service provider).
- Do not reply to abusive or worrying text or video messages - your Mobile service provider will have a number for you to ring or text to report phone bullying. Visit their website for details.

Email

- Never reply to unpleasant or unwanted emails.
- Don't accept emails or open files from people you do not know.

- Ask an adult to contact the sender's ISP by writing abuse@ and then the host, eg.abuse@hotmail.com.

Web

- If the bullying is on the school website, tell a teacher or parent, just as you would if the bullying was face-to-face.

Chat Room & Instant Messaging

- Never give out your name, address, phone number, school name or password online. It's a good idea to use a nickname. Do not give out photos of yourself either.
- Do not accept emails or open files from people you do not know.
- Remember it might not just be people your own age in a chat room.
- Stick to public areas in chat rooms and get out if you feel uncomfortable.
- Tell your parents or carers if you feel uncomfortable or worried about anything that happens in a chat room.

Think carefully about what you write - don't leave yourself open to bullying

REMEMBER: Always tell an adult

Appendix 4: Online Safety Training Needs – Self-Audit for Staff

Adapt this audit form to suit your needs.

Online Safety Training Needs Audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	

Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 5: Online Safety Incident Report Form

Pupil Name:	**Class:**
Date of Incident:	**Time of Incident:**
Reporting Staff:	**Witness:**

DSL Notification Date:

Where did the incident occur?

☐ In school / service setting
☐ Outside school / service setting

Who was involved in the incident?

☐ Child / young person
☐ Staff member
☐ Adult
☐ Other (please specify)

Type of Incident

☐ cyber bullying or harassment
☐ deliberately bypassing security or access
☐ violence
☐ profanity
☐ grooming
☐ online radicalisation
☐ sexual images
☐ hacking or virus propagation
☐ child abuse images
☐ terrorist material
☐ online gambling
☐ racist, sexist, homophobic, transphobic, bi-phobic, religious hate material
☐ soft core pornographic material
☐ illegal hard-core pornographic material

Accidental Access (check one):

Incident involved material being:

☐ created
☐ viewed
☐ shown to others
☐ printed
☐ transmitted to others
☐ distributed

Deliberate Access	
Incident involved material being: ☐ created	Could the incident be considered as: ☐ grooming ☐ cyberbullying

☐ viewed ☐ shown to others ☐ printed ☐ transmitted to others ☐ distributed	☐ Harrassment ☐ Breach of Acceptable Use Policy ☐ Other (please specify):

Description of the incident:

How was the content accessed?

- ☐ School internet
- ☐ via a PC/laptop
- ☐ via a tablet
- ☐ via a mobile phone
- ☐ via email
- ☐ Via an internet browser
- ☐ via a social media website
- ☐ via an app

What action was taken in relation to those involved in the incident?

What action was taken regarding the site/content accessed?

Outcome of Investigation:

What follow-up action was taken?

- ☐ Referral to LADO
- ☐ Referral to Children's Social Care
- ☐ Advice to parents
- ☐ Police investigation
- ☐ Other (please provide details):