Anti-Cyber Bullying Policy

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