St. James' Church of England Primary School

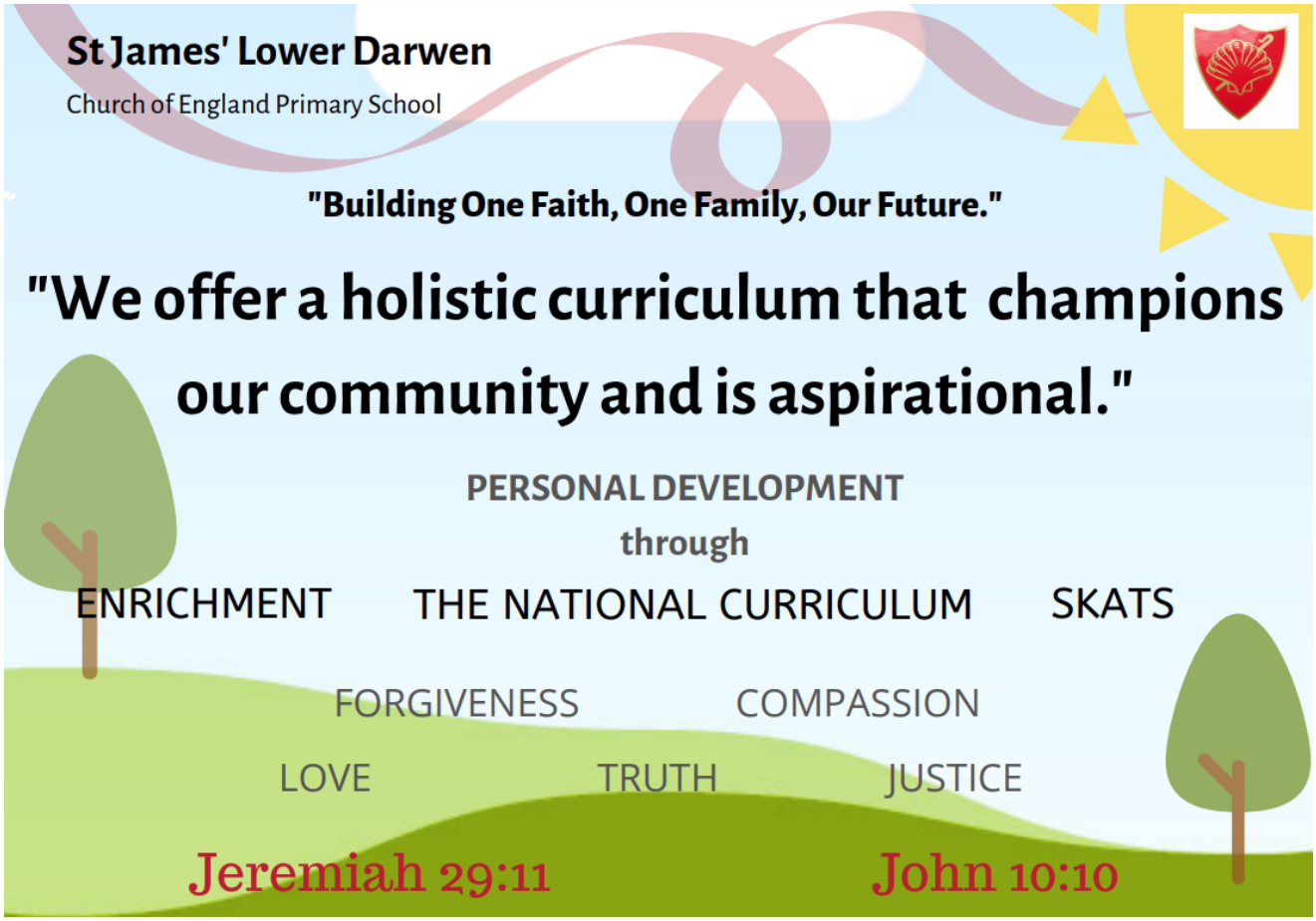
'Building One Faith, One Family, Our Future'

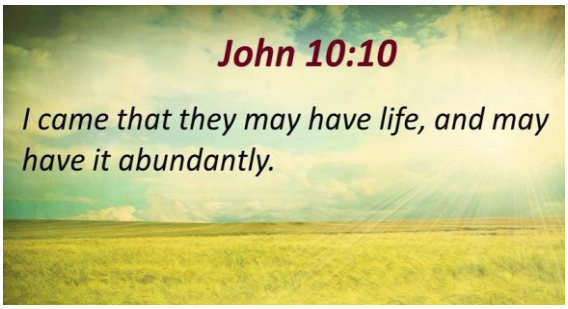
Online Safety Policy

Written by Lesley Jacques – Autumn 2024
Approved by Governors – Autumn 2024

Review Date: Autumn 2026 (Resources Committee)

Foundation, Vision and Intent





We want our children to know that **God has a plan for them** that means **they live their best life possible.**

Each **policy** and procedure within school, alongside the ongoing **curriculum** delivery, our **SKATS** programme, **enrichment** and the **spiritual development** offered to our families through Worship, RE and our links with Church, work towards making this happen.

Aims

Our school aims to:

- have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors;
- 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, radicalization and extremism.
- **contact**: being subjected to harmful online interaction with other users; for example: child on child 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 non-consensual 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/)/

Legislation and Guidance

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers all stakeholders to protect and educate pupils and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

This policy is based on the Department for Education's (DfE) 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;
- 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 cyberbullying 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.

Roles and Responsibilities

The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Jacqui Buckley.

All governors will:

- ensure that 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.

The Headteacher

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

The Designated Safeguarding Lead

Details of the school's DSL are set out in our child protection and safeguarding policy as well relevant job descriptions.

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

- supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- working with the headteacher, ICT technician (NYBBLE Ltd) and other staff, as necessary, to address any online safety issues or incidents:
- ensuring that any online safety incidents are logged (see appendix) 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;
- updating and delivering staff training on online safety (appendix 4);
- 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.

The ICT technician- Compuserv Ltd

The ICT technician is responsible for:

- putting in place appropriate filtering and monitoring systems - Talk Straight Schools Broadband, 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 monthly basis;
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- Liaising with the Designated Safeguarding Lead around filtering systems.

- ensuring 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.

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, and ensuring that pupils follow the school's terms on acceptable use;
- working with the DSL 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.

Parents

Parents are expected to:

- notify a member of staff or the headteacher of any concerns or queries regarding this policy;
- ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

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 3).

Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum that has been supported by the Teaching Online Safety in School. From September 2020 all schools will have to teach relationships education and health education in primary schools.

In Key Stage 1, pupils will be taught to:

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

Pupils in Key Stage 2 will be taught to:

- use technology safely, respectfully and responsibly;
- recognise acceptable and unacceptable behaviour;
- identify a range of ways to report concerns about content and contact.

By the end of primary school, pupils will know:

- that people sometimes behave differently online, including by pretending to be someone they are not;
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous;
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them;
- how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met;
- how information and data is shared and used online;
- 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.

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 or virtual learning environment. Online safety may be covered in parents' evenings. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL and/or headteacher. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

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 Positive Behaviour Policy.)

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

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 Positive Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavors to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

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. 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.

Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. 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. The computing lead and SLT have formed a detailed overview for the safe and secure access of the Internet. This can be found in the subject section of the school website.

Governors ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. This is done weekly by way of an external report from the Local Authority, as per the KCSIE para. 141.

Pupils Using Mobile Devices in School

Pupils may not bring mobile devices into school.

Any use of mobile devices in school by pupils will result in the device being confiscated until home time.

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.

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.

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 headteacher.

Work devices must be used solely for work activities.

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 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 school's 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.

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.

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.

Monitoring Arrangements

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

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the governing board.

Links with Other Policies

This online safety policy is linked to our:

- Safeguarding Children & Child Protection Policy
- Computing Policy
- Positive Behaviour Policy
- Data Protection Policy
- Staff Code of Conduct Policy
- Complaints Policy
- Acceptable Use Policy and ICT security Policy