SAINT JAMES'
Church of England School
Nursery & Pre School

LDST
Liverpool Diocesan Schools Trust

Online Safety Policy

This policy has been adopted by the governing body of St James CofE Primary School.
It will be reviewed annually or as required. If you require more information, please contact the school office.

St James' CofE Primary School
Equality Policy

Mission Statement

Through him we learn to live abundant lives, especially treasuring the values of friendship, trust, thankfulness, respect, forgiveness, hope and courage.

Vision Statement

Walking hand in hand with Jesus, fulfilling the potential God has given us.

Luke 1:37 'For with God nothing shall be impossible.'

Mission Aim

At St James' CofE Primary School, the Christian (and indeed, inclusive human) values "friendship, trust, respect, forgiveness, hope and courage" inform our whole life together.

This policy reflects the Equality Act 2010 which harmonises and replaces previous legislation including the Race Relations Act 1976, Disability Discrimination Act 1995, Gender Recognition Act 2004 and Sex

Key people

St James' CE Primary School	Designated Safeguarding Lead (DSL)	Jackie Moore
	Deputy Designated Safeguarding Leads	Leila Abrams Teresa Gaffney Judy Swann Michaela Dillon Danielle Major
	Computing Lead	Gemma Gaskell
	Online safety / safeguarding governor	Sam Rusling Joel Thornton
	Date this policy was reviewed and by whom	October 2020
	Date of next review and by whom	To be reviewed annually

Purpose

Developing technology, including information technology, brings many opportunities to improve our lives and communication; however, it also brings risks and potential dangers to children and young people in particular. This policy sets out how we strive to keep children safe when using technology while they are in school and how we educate children, and the adults responsible for them, about the potential risks of using IT when at home. This policy takes account of the advice offered by the Local Authority, the LDST, the NSPCC and Keeping Children Safe in Education 2019.

Keeping Children Safe in Education states that the breadth of issues within online safety can be categorised into three areas of risk:
• content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
• contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults;
• conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

The following are some examples of the risks presented to children when using IT:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to/loss of/sharing of personal information.
- The risk of being 'groomed' by people they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication /contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable electronic/Internet games.
- Plagiarism and/or copyright infringement, including making illegal downloads.
- Child Sexual Exploitation
- Radicalisation

Roles and responsibilities

The head teacher is responsible for:

- ensuring the safety (including e-safety) of all members of the school community, through the full and correct implementation of all relevant policies and procedures;

- ensuring that e-safety education is provided to our pupils regularly and appropriately, with the support of the IT and computing technician;
- ensuring that the correct procedures are followed in the event of a serious e-safety allegation being made against a member of staff;
- ensuring that training and advice on e-safety are provided to all staff and governors on a regular basis and at least annually;
- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident;
- ensuring that parents/carers agree to ensuring the safe use of IT by their children, both at school and at home, as part of the home-school agreement;
- reporting any serious issues as appropriate, in line with this or other relevant school or Local Authority policies and protocols and keeping the buddy governor for child protection informed of these.
- Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are aware
- line management of and liaison with the school IT and computing technician, as necessary;

The IT and computing technician is responsible for:

- ensuring that the school's IT systems and hardware are secure and not open to misuse or malicious attack;
- ensuring that the school's acceptable use agreements are signed by all users of the school's IT systems before use and keeping a record of these;
- ensuring that users may only access the school's networks through a properly enforced password protection policy;
- ensuring that shortcomings in the infrastructure are addressed and if necessary reported to the school business manager so that appropriate action may be taken;
- considering and acting on any issues relating to school filtering or other e-safety issues and how they should be dealt with, including keeping a log of any such incidents;
- reporting any serious issues to the designated person or deputy designated person for child protection ;

The school business manager is responsible for:

- management of purchases related to e-safety.

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and procedures;
- they have read, understood and signed the school's acceptable use agreement/s for staff ;
- they report any suspected misuse or other e-safety problem to the designated safeguarding lead.
- any digital communications with pupils are on a professional level and only carried out using official school systems;
- they teach e-safety to all pupils, including those with SEN or other vulnerabilities, at every opportunity, through the curriculum and other relevant school activities.

The governing body is responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors' health and safety committee at its annual meeting and through the buddy governor for child protection receiving regular information about e-safety incidents and monitoring reports.

School e-safety procedures

Acceptable use agreements

All members of the school community are responsible for using the school IT systems in accordance with the appropriate acceptable use agreement, which they will be expected to sign before being given access to school systems.
Acceptable use agreements are provided for:

- **Pupils (EYFS + KS1/KS2)** – a list of E-Safety rules (Appendix I and II), which they must sign and/or have countersigned by a parent/carer at the time when they enter our school. Children cannot access school information technology without the safety rules being signed. The parents' agreement also includes permission for their child to use the school's ICT resources (including the internet) and permission to publish their work.
- **Staff members** – a general 'acceptable use' agreement (Appendix III), which is informed by guidance documents provided by the Local Authority (Appendices IV, V and VI) plus separate agreements (Appendix VII) for using pen drives and for laptop and/or I-Pad

loans, which have specific guidance and acceptable use agreements, which must be signed before use. Staff sign when they take up their role in school and in the future if significant changes are made to the policy.

- **Students//Supply staff** – these must sign relevant documents as for staff members when they take up their period of training. They will be given their own student/supply log in. Students have a meeting with the safeguarding leads to go through the Safeguarding policies.
- **Volunteers** – it is not usual for volunteers to have access to computing or other IT equipment in school. If this is likely to be asked of them or if requested by them, the headteacher, school business manager or IT and computing technician must be consulted and relevant documentation can then be provided.

E-safety incidents

- Pupils are protected from abuse whilst using school-based technologies by an approved filtering service from an outside provider. See Computing Policy. If any incident occurs that compromises a pupil's safety or well-being through their use of IT, this is logged on CPOMS.
- Pupils should be made aware of how to report any threat to their safety/well-being, or any other concern related to their IT or online usage. This may be through a direct verbal complaint/report to a member of staff or through our 'report an issue' on the school website. Incidents reported to a staff member must be logged using CPOMS. Appropriate follow-up action must then be taken.
- Staff members are equally protected from abuse by the above systems; this includes filtering of emails within school. Any misdemeanours should be reported to the DSL or the chair of governors.

Management of still or moving images

- All parents/carers are asked to sign their agreement to school's use of images internally, on the website or as part of wider publicity. Where necessary, this is re-confirmed for any event that may include photography or film, via an 'opt-out'.
- School maintains and gives full regard to a list of any and all pupils for whom permission has not been given.

St James' CofE Primary School

- Images are stored securely on the school server and currently are retained for the purpose of any legitimate use by school eg commemoration events.

Technologies and understanding

- At Saint James' we try to allow all pupils to have access to a wide range of IT/computing devices for multiple purposes. Allowing pupils to gain a broad and varied experience in technological aspects will help to progress their understanding and development of computing technologies.
- Pupils have supervised access to many devices, but are not limited only to these, as new and appropriate technologies are being developed all the time. Current devices include: laptops, desktop computers, iPads and Kindles.
- At St James' we do not permit the use of social media in school, nor promote their use by children. Facebook and Twitter are used by designated staff to communicate news and messages to parents/carers. See social media policy. No communication by pupils is permitted with unknown persons, including the use of webcams or video conferencing.
- Lessons involving IT are monitored and observed strictly and thoroughly to maintain child safety and to comply with our e-safety rules. The e-safety rules that are given to parents/carers to be completed by themselves and their children will be complied with by staff when planning any computing lesson or a lesson involving the use of IT.
- All digital devices needed for learning are provided by school, therefore no personal devices are used in school, unless for approved event such as BYOD ('bring your own device'). Prior to such events, written parental consent will always be obtained before any related lesson takes place. No staff or children are permitted to have their mobile phones in school, and such devices should not be brought in school by pupils. Mobile devices belonging to staff and adult visitors to school are stored in the office areas, either in staff lockers or in the safe keeping of office staff. If a pupil brings a mobile into school, for whatever reason, it is also stored in this area throughout the day and released back to the pupil before they go home.

E-Safety education

Pupil training

The education of pupils in e-safety is an essential part of the school's e-safety provision and actively protects their mental health and well-being whilst online. Children and young people need

the help and support of the school to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.
E-safety education will be provided in the following ways:

- Elms Computing Consultancy are currently supporting teachers to strengthen their subject knowledge in Computing. Elms Computing Consultancy are currently teaching each year group for one hour a week. This includes teaching E safety throughout each lesson.
- A planned e-safety programme is provided by Elms Consultancy as part of Computing, PHSE and other lessons and should be regularly revisited – this will cover both the use of Computing and new technologies in school and outside school
- We use the resources on CEOP's Think U Know site as a basis for our e-safety educationhttp://www.thinkuknow.co.uk/teachers/resources/
- Key e-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils should be helped to understand the need to use their personal pupil credentials for accessing the school's network and encouraged to adopt safe and responsible use of IT both within and outside school.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff must be vigilant in monitoring the content of the websites the young people visit.
- Members of staff must act promptly and appropriately in dealing with any unsuitable material found accidentally by a pupil in internet searches, and report such incidents using the e-safety report form.
- An annual 'Internet Safety Day' takes place in the spring term, as a way of highlighting the importance of staying safe when using information technology.

Pages with a wealth of information for children and parents can be found below:

Support for children

• Childline for free and confidential advice

• UK Safer Internet Centre to report and remove harmful online content

• CEOP for advice on making a report about online abuse

- The school website has a variety of resources to support children with online safety https://www.saintjames.wigan.sch.uk/online-safety/

Parental support

• Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support

• Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents

• Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying

• Government advice about security and privacy settings, blocking unsuitable content, and parental controls

• Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world

• Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation

• London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

• Lucy Faithfull Foundation StopItNow resource can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)

• National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online

• Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games

• Parentzone provides help for parents and carers on how to keep their children safe online

• Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations

• UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

- The school website has a variety of resources to support parents with online safety https://www.saintjames.wigan.sch.uk/online-safety/

Home learning

Home learning is completed using 'Seesaw' - Student driven digital portfolios and simple parent communication. Children and parents have had to sign a user/parent agreement to use this. They have their own passwords and login. Children's work is made confidential so that only the class teacher can view it.

Staff follow the 'Remote Learning Policy'. Our remote learning policy seeks to ensure that we provide high-quality teaching and learning in the event of (i) single pupil self-isolation (ii) classes, year groups or 'bubbles' being required to work at home, or (iii) whole school closure due to Covid-19.
Seesaw's privacy policy, data and safety security can be accessed below
https://www.esafety.gov.au/key-issues/esafety-guide/seesaw

Staff training

It is essential that all staff also receive e-safety training and understand their responsibilities, as outlined in this policy. Training is offered as follows:

- A planned programme of e-safety training, available to all staff. Elms Computing Consultancy are currently supporting teachers to strengthen their subject knowledge in Computing.
- E-safety training as part of the induction programme for new staff, ensuring that they fully understand the school e-safety policy and acceptable use policies, which are signed as part of their induction.
- An audit of the e-safety training needs of all staff, carried out regularly, with an expectation that some staff will identify e-safety as a training need within the performance management process.

- Regular updates for key staff, provided through attendance at local authority or other information /training sessions and by reviewing guidance documents released by the DfE, local authority and others.
- All staff have accessed the Prevent Duty training through the following website http://course.ncalt.com/Channel_General_Awareness/01/index.html.
-

Governor training

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any subcommittee or group involved in Computing, e-safety, health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority (Governor Services or Learning and Achievement Service), National Governors Association or other bodies.
- Participation in school training/information sessions for staff or parents

Parent and carer awareness raising

St James'
CofE Primary School

The school seeks to provide information and awareness to parents and carers through:

- Letters, newsletters and school website, Facebook and Twitter;
- Parents' evenings;
- Reference to the parents materials on the Think U Know website (www.thinkuknow.co.uk) or others.
- The school website has a variety of resources to support parents with online safety https://www.saintjames.wigan.sch.uk/online-safety/

Policy Scope

- This policy applies to all members of the school community who have access to and are users of school IT systems, both in and out of school.
- The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

Links to other policies

This policy has strong links to other school policies as follows:
Computing Curriculum
Social Media policy for Employees in Schools
Safeguarding and child protection
Mental health and well-being
Behaviour management
Anti-bullying
Remote Learning Policy

Policy development, monitoring and review

This e-safety policy, or aspects of it, have been developed by a working group made up of:

- The headteacher and the IT and computing technician;
- Teaching and support staff;
- Governors, including parent governors;
- Pupils.

The implementation of this e-safety policy will be monitored by the headteacher and the IT and computing technician, with the governing body.
The governing body will receive a report on the implementation of the policy (which will include anonymous details of any e-safety incidents) at regular intervals, at least annually.

TRUST THANKFULNESS RESPECT FORGIVENESS HOPE COURAGE
St James' CofE Primary School