THE SPIRE
CHURCH OF ENGLAND LEARNING TRUST
collaborate . learn . achieve

Online Safety Policy 2023-2024

Adopted by

St Matthias CE Primary School

This policy is reviewed/updated by Ginnie Beale (The Spire Academy Safeguard Lead) and James Thompson. This is approved annually by the Trust for adoption by the Trust Schools.

Reviewed: June 2023

Next Review: June 2024

In collaboration with

Computing and the use of digital devices is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Computing and ICT covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of technology and computing within our society as a whole.

Whilst exciting and beneficial all users need to be aware of the range of risks associated with the use of these technologies.

At The Spire Church of England Learning Trust (The Trust) we understand the responsibility to educate our pupils on online safety; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of fixed and mobile internet technologies provided by the Trust and/or school. Any visitors using their own devices within school sign on entry to say that they adhere to the Trust's Acceptable Use Agreement and this online safety policy.

Roles and Responsibilities

As online safety is an important aspect of strategic leadership within the school, the Trust, Head and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

Within each setting within the Trust, the DSL has overall responsibility for online safety; they can be supported by appropriately trained deputies and should liaise with other staff as appropriate, but this responsibility cannot be delegated.

The named staff supporting the DSL in each setting are listed below:

St John's CE Middle School Academy

- Computing Lead; Ben Clements
- Online Safety coordinator; Ben Clements
- PSHE Lead; Aoife Kelly
- IT Manager Sean Chadwick
- IBS Schools for internet filtering.

St John's CE Primary

- Computing coordinator; Charlotte Shepherd
- Online Safety coordinator; Charlotte Shepherd
- IT Manager; Sean Chadwick
- Netbuilder for internet filtering

St Matthias CE Primary

- Computing coordinator; James Thompson
- Online Safety coordinator; James Thompson
- IT Manager; Sean Chadwick
- IBS Schools for internet filtering

Witton Middle School

- Computing coordinator; David Palmer
- Online Safety coordinator; David Palmer

- IT Manager; Sean Chadwick
- CoConnect for internet filtering

This policy, supported by the Trust's acceptable use agreement, is to protect the interests and safety of the whole school community.

Requirements as set out in Keeping Children Safe in Education. Full detail can be found in the school safeguarding policy.

- DSLs will access appropriate training and/or support to ensure they understand the unique risks associated with online safety, can recognise the additional risks learners with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep children safe online.
- All staff will be provided with online safety information and training at induction
- All staff will receive online safety training as part of regular (at least annual) child protection training
- Staff will receive updates on online as required
- Children will be taught about online safety, including as part of statutory Relationships and Sex Education (RSE)
- The individual schools within the Trust recognise that a one size fits all approach may not be appropriate and a more personalised or contextualised approach for more vulnerable children e.g. victims of abuse and SEND, may be needed.
- We recognise that child on child abuse and child on child sexual violence and sexual harassment can occur online. Full detail can be found in the school's Anti-bullying policy.
- DSLs from all schools within the Trust will ensure they have accessed the UKCIS 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' guidance and are familiar with its content and when it should be followed.

Managing the school's online safety messages

We endeavour to embed online safety messages across the curriculum whenever the internet and/or related technologies are used. These messages will be appropriate to the age and development of the children being taught.

Online safety guidelines and the SMART rules will be prominently displayed around the school and referred to as appropriate.

As a school, each year, we also participate in online safety activities during Safer Internet Day.

Online safety in the Curriculum

The school provides opportunities within PSHE and Computing lessons to teach about online safety.

Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise as well as the Computing and PSHE curriculum.

The teaching of online safety focuses on helping children to recognise inappropriate content, conduct, contact and commerce and helps them learn how to respond or react appropriately.

Pupils are made aware of the impact of online bullying and how to seek help if they are affected by these issues.

Pupils are taught how to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.

Security, Data and Confidentiality

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the Trust's/school's e-safety Policy.

When accessing, amending and saving any data or information, relating to the school or pupils, school staff follow the guidelines set out in the General Data Protection Regulations (2018.)

Managing the Internet

All internet activity within school is monitored and filtered through IBS Schools Smoothwall cloudbased system and Impero. Whenever any inappropriate use is detected, the ICT Manager is notified and the incident will be followed up in line with the school Acceptable Use Policy and Safeguarding reporting procedures.

The school maintains Pupils will have supervised access to Internet resources (where reasonable) through the school's digital devices. If Internet research is set for homework, staff will remind Pupils of their online safety training. Parents are encouraged to support and supervise any further research.

Infrastructure

Our internet access is provided by Chestnut Business and monitored by IBS Schools and the IT Manager. The IT Manager manages the administrative devices throughout school and curriculum access also managed by the IT Manager.

Staff and pupils are aware that should they encounter or access anything unsuitable or damaging they must report it immediately to teachers, online safety co-ordinator, the IT Manager or the DSL.

Mobile and Smart Technologies

Personal Mobile devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use during designated times and locations outside of the classroom. These are **not** to be used at any time whilst children are present.

Where personal mobile devices have access to the internet via the schools Wi-Fi network, they are filtered down to the same restrictions as pupils.

The school is not responsible for the loss, damage or theft of any personal mobile device.

Within the Trust settings catering for older pupils, mobile phones may be brought to school. In Appendix 1 the school specific information can be found.

Managing email

The use of email within school is an essential means of communication for staff. Pupils currently do have access to individual email accounts within school, however there are policies in place to restrict sending and receiving emails. Pupil email accounts are used to access Teams which can be monitored by the teachers and Deputy Head where concerns are raised.

Staff must use the school's approved email or communications system for any school business rather than personal accounts.

Staff must inform (the online safety co-ordinator/ line manager/ IT Manager/DSL) if they receive an offensive or inappropriate e-mail.

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 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 or relevant agencies.

Facebook/Social Media Groups

It is not acceptable to publicly criticise or blame school management and colleagues at any time; especially through any social media including internet "blogs", websites or social networking tools such as Facebook or Twitter and you must be aware that the laws governing defamation, breach of copyright, etc. apply equally to "blogging" as to other forms of communications.

Offensive, defamatory, discriminatory or otherwise inappropriate comments will not be tolerated and may constitute a disciplinary and/or criminal offence, as could the disclosure/publication of any confidential or personal information about the school, its staff, pupils or other members of the school community.

Safe Use of Images

Creation of videos and photographs

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

All staff are aware of specific children (they have responsibility for) in school who do not have photograph permissions. If they do have permission, staff are aware of which platforms they can be used on.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes field trips. The school's own mobile devices must be used in this case.

Publishing pupil's images and work

All parents/guardians will be asked to give permission to use their child's work/photos in publicity materials or on the school website, twitter account or mobile app.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.

Parents/ carers may withdraw or amend permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa on the school website, twitter account, mobile app or any other school based publicity materials.

Storage of Images

Images / films of children are stored securely on the school server and / or teacher's individual encrypted devices for the length of time the pupil remains at the individual Trust Schools, this will vary from school to school.

Misuse and Infringements

Complaints

Complaints or concerns relating to online safety should be made to the online safety coordinator, line manager, IT Manager or DSL

Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the online safety coordinator, IT Manager or DSL.

Deliberate access to inappropriate materials by any user will lead to the incident being logged, in the first instance, by the IT Manager and then forwarded to the Online Safety Lead or DSL. Depending on the seriousness of the offence; investigation may be carried out by a member of the Senior Leadership Team. Staff are aware, as outlined in the staff code of conduct, that negligent use or deliberate misconduct could lead to disciplinary action.

Appendix 1

Mobile Phone and Smart Technology at St Matthias'

Schools within the Trust recognise that mobile phones are a part of everyday life and, for parents who choose to allow their children to bring mobile phones to school, the following policy will apply. All pupils bringing mobile phones to school require parental permission.

Responsible Use

Year 6 pupils are only allowed to use mobile phones at the end of the school day once they have left the premises. Pupils will not be allowed to use phones on school premises before school or at any time during the school day.

Pupils will be responsible for their own phones and whilst the Governors give permission for phones to be brought to school, they will not take any financial responsibility for phones that are lost, damaged, stolen or confiscated.

Pupils must ensure that files stored on their phones do not contain any inappropriate material. Pupils who fail to follow this will have their phone confiscated and both their parents and the police will be informed.

Cyber-bullying is completely unacceptable. Pupils involved in this will have their phone confiscated; it will be returned to their parent/guardian, or passed to the police depending on what has been reported. The consequence for this offence could result in serious consequences. Additional detail can be found in the anti-bullying policy, safeguarding policy and Behaviour and relationships policy.

Phones must be switched off (not just on silent) and out of sight at all times and kept in the Year 6 cupboard whilst on the school premises.

Checks and investigation will be carried out where reports are received of Pupils using their phones while in school.

Where Pupils do not follow this expectation, which is in place for safeguarding reasons and to ensure that learning is not disrupted, the phone or smart device will be confiscated. On the first occasion the phone or smart device may be collected by the student at the end of the day. On any subsequent occasions the phone will be held at reception until collected by the parent/guardian.

Pupils who do not follow this expectation for a third time will not be permitted to bring the phone or smart device for a given amount of time.

If there is a genuine **emergency** which required communication with home, Pupils will continue to be able to use the phone in reception as previously and not their mobile phones.

Parents should continue to phone reception in order to contact their children in a genuine **emergency** and any messages will be given to the student. Please do not try to communicate with your child during the school day via their mobile phone.

Pupils need to acknowledge that it is a privilege to be permitted to bring mobile phones to school and non-adherence to this policy will lead to a removal of this privilege.

This policy has been devised in order to protect all children and staff within the Trust's schools from any form of abuse through the misuse of mobile phones and we would appreciate your full support with this.

Appendix 2

Online Safety - Information and support for parents and children

There is a wealth of information available to support children, parents and carers to keep safe online. The following list is not exhaustive but should provide a useful starting point:

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

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

Appendix 3

Amendments made during review June 2023 – to assist author with next review

Page no	Heading	Text approved
Page 4	Mobile and Smart Technologies – personal mobile devices	The school allows staff to bring in personal mobile phones and devices for their own use during designated times and locations outside of the classroom. These are **not** to be used at any time whilst children are present.