Online Safety Policy

Policy reviewed: September 2020

'St John's Angell Town CE Primary School is committed to the safeguarding and the wellbeing of all our pupils'

Vision Statement

Making the world a better place through faith, hope and love.

Mission Statement

Christian values and high expectations are at the heart of all aspects of our school life, providing a safe, happy and inclusive learning environment where children are encouraged to develop respect, self-esteem and confidence. We aim to find exciting ways to educate, making use of the latest developments in technology.

At St john's Angell Town CE Primary School (SJAT) we celebrate success and encourage everyone to achieve their full potential, by working together in partnership with parents, carers, the Church and wider community.

Introduction

As an increasingly digital world develops, within our School w, e encourage the pupils' use of the rich information and communication resources available through the internet, together with the development of appropriate skills to analyse and evaluate these resources. While technology is unlikely to be the same by the time our pupils leave secondary school, this will enable fundamental skills to be developed to support successful citizenship.

The school recognises and embraces the powerful tool of technology, and as such we strive to ensure our pupils have good, appropriate and safe access. However, the school also recognises its responsibilities in ensuring safe use of the internet and other communication systems for all pupils and so this policy outlines our strategy to protect pupils. This policy has been written in conjunction with the statutory requirements and guidance found in Keeping Children Safe in Education 2020.

Pupil Protection

It is our intention to protect our pupils from inappropriate or undesirable material. The following criteria define inappropriate or undesirable materials:

- Obscene, offensive, illegal, inaccurate or discriminatory
- Pupils should not feel or become uncomfortable, threatened or worried by material or information on websites, email or other online forums.
- Similarly, pupils must not harass, insult, attack others, violate copyright, or trespass in others' folders
- Illegal, inappropriate, inaccurate, harmful or discriminatory material
- Pupils should not feel or become uncomfortable, threatened or worried by material or information on websites, email or other online forums, exposed to commercial advertising, or adults posing as children or young adults
- Personal online behaviour that increases the likelihood of, or causes harm, for example making, sending and receiving explicit images, online bullying
- Pupils should not violate copyright or trespass in others' folders

In addition, the school will never make publically available photos or videos with the names of individual children. Where photographs or videos are used in published materials, including the school website or other areas, the school will ensure:

Parental permission is given

Photographs or videos of groups of children will be described as "children investigating a science problem", for example.

Parental permission will be sought to share photos and comments on private online platforms such as Class dojo.

Internet Access/Filters

- Access to the internet is possible via the computer network, using computers (including tablets) and Interactive whiteboards (IWBs).
- There is a bank of laptops in the ICT for use in the suite or throughout the school. In addition, there are PCs in various offices, and laptops linked to IWBs in each classroom.
- A bank of iPads is also available, which must be collected and returned by staff only.
- All computers linked to the internet incorporate automatic anti-virus protection.
- Pupils must not bring in software from home to upload onto the system.
- The broadband internet connection is provided by LGFL and incorporates a filtering system or "firewall" appropriate to the age of our pupils, which screens undesirable sites at a proxy server.
- The children will be shown how to use Hector's World Safety Button, the child activated safety tool which they can use if something on the screen upsets them.
- Children should not use their own equipment, such as mobile phones, to access the internet as the filtering in place may not be deemed adequate for the school environment and content accessed cannot be monitored by the school systems. Mobile phones will be stored securely in the office during the school day.

Guidelines for in school use of the Internet with pupils

The Computing subject leader has overall responsibility for ensuring that skills are planned into the curriculum in line with National Curriculum expectations and made specific in long term planning. Internet access is integrated into learning activities at the planning stage across the school.
Where applicable, suitable websites to support learning are identified by all staff and are identified on planning and can be bookmarked for later use.
Children are also able to use specified search engines such as "Google" to find appropriate websites – to ensure appropriate content is returned in these searches, children are taught to include terms such as 'for kids' or use child-safe search engines.
Our website will provide links to safe websites which are appropriate for the age phase being taught, as well as current topics. For online tools children will be provided with login information.
The use of social networking sites are not permitted in the school. Children are advised against the risks of social media and the importance of age restrictions.

Supervision/responsibility

It is critical that responsible usage of the internet to all pupils is taught in specific detail in Computing and other lessons (including PSHE, P4C and in assemblies). Children will be reminded of their responsibility each time they use a device. Therefore, children are only allowed to access the internet once they have been given consent from a member of staff. This applies to lesson times, break times and before/after school.

However, due to the nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. Neither the school nor LGFL can accept liability for the material accessed or any consequences thereof.

It is important to note the shared responsibility of all stakeholders to ensure safe usage. Further information on using ICT safely, potential misuses and reporting procedures can be found in the Child Protection and Safeguarding policy.

Misuse of the Internet

Misuse of the Internet will not be tolerated. In the first instance, the class teacher should deal with any misuse of the internet with the child. However, the incident must always be reported to the Computing Leader and will be logged in the child's behaviour log.

Should there be any concerns over the types of material accessed (e.g. types of materials identified earlier in this policy), the matter should immediately be reported to the Headteacher. The sanctions imposed will reflect the severity of the

incident. These could range from the Headteacher contacting parents, to a temporary suspension of ICT rights, to permanent exclusion for very serious offences.

Pupils must report accidental access to inappropriate material immediately to their teacher.

Promoting Fundamental British Values, and Preventing Radicalisation and Violent Extremism

Our School values the fundamental rights of freedom of speech, expression of beliefs and ideology and understanding of others which are the core values of our democratic society. However, all rights come with responsibilities and free speech or beliefs designed to manipulate the vulnerable or which advocate harm or hatred towards others will not be tolerated.

Our School seeks to protect its children and staff from all messages and forms of violent extremism and ideologies including those linked to, but not restricted to, the following: Far Right/Neo Nazi, White Supremacist ideology, extremist Islamic ideology, Irish Nationalist and Loyalist paramilitary groups and extremist Animal Rights groups.

Our School is clear that exploitation and radicalisation will be viewed as a safeguarding concern and will be referred to the appropriate safeguarding agencies. For further information, refer to the Department for Education (DfE) Prevent guidance, our statement of British Values and Safeguarding and Child Protection policies.

Home Learning

Staff at The School will consider the safety of the children at their school when they set home learning tasks online. When planning online lessons/activities The School staff will follow all relevant guidance received from the DfE and the Local Authority and will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.
The School will be ensure children who are being asked to work online have very clear reporting routes in place so they can raise any concerns whilst online. For example, talking to the adult in class or raising an issue on Seesaw.
As well as reporting routes back to The School, the school will also signpost children to age appropriate practical support from the likes of:

- **Childline** - for support
- **UK Safer Internet Centre** - to report and remove harmful online content
- **CEOP** - for advice on making a report about online abuse.

The School will be in regular contact with parents and carers to reinforce the importance of children being safe online. It will be especially important for parents and carers to be aware of what their children are being asked to do online.

Advice to parents and carers on keeping pupils safe online during home learning.

Supporting good behaviour ensures a productive online learning environment for all of our learners.
Children are expected to join the remote lessons on time (with the exception of those who are unable to do so for good reason e.g. living in a different time zone, if abroad for any authorised reason) and behave with respect and courtesy throughout the lesson.

All our teachers follow the Whole School Behaviour Policy with regard to discipline and classroom management. Rules and routines are discussed with learners so that they are understood clearly. During home learning, it is important to help your child stay safe online when they are using existing devices and services or when they are using new services, apps or devices, such as webcams and tablets, to access the set work. Therefore, to support this it is vital that you:

Check security and privacy settings

- Adjust privacy and safety settings increases security and controls the personal data you/your child shares. Look for the 'privacy and security' or 'settings' on the app or website.
- Review the security settings on your/your child's smart' devices. If your/your child's device is using a default or easily guessable password, change it.
- Set up two-factor authentication. This is a free security feature to stop unwanted people getting into your/your child's accounts. You/your child will receive a text or code when you/they log in to check you/they are who you/they say you are.
- Update your/your child's devices because using the latest version of software and apps can immediately improve your/your child's security.

Block unsuitable content

It is important to understand the website or app your child is using and how they (website or app) do things - find out in their terms and conditions.

If you/your child sees harmful activity, report it to the site. Platforms often offer advice on how to do this but you/your child can also seek support at:

- Samaritans
- Mind
- BEAT

To prevent unwanted content from appearing, set filters on your home broadband and mobile networks. The UK Safer Internet Centre has advice on how.

Protect against Fraud

Criminals will use every opportunity they can to scam innocent people. Beware of fraud and scams online eg: phishing emails and text messages. There is guidance on how to recognise these emails.

You/your child can forward any suspicious emails to report@phishing.gov.uk, a new service run by the National Cyber Security Centre (NCSC) Suspicious Email Reporting Service. The NCSC's automated programme will immediately test the validity of the site and if found to be phishing scams, they will be removed immediately.

Do not give out your/do not let your child give out, personal information to websites or in response to emails/text messages you/they do not recognise or trust.

If you think you/your child has been scammed, defrauded or experienced cyber-crime **Action Fraud** is the UK's national reporting centre for fraud and cybercrime.

Check the facts

Not all information online is reliable. Before your child likes, comments or shares something online they need to use the SHARE checklist to make sure they're not contributing to the spread of harmful content:

- **S**ource - make sure information comes from a trusted source
- **H**eadline - always read beyond the headline
- **A**nalyse - check the facts
- **R**etouched - does the image or video look as though it has been doctored?
- **E**rror - look out for bad grammar and spelling

The SHARE checklist can help you understand and spot disinformation and **NewsGuard** has a free tool to help the public identify fake news.

Take breaks

Make sure that your child takes regular breaks from their screens. There are a range of tools available to help you manage their screen time:

Apple's Screen Time
Google's Family link

Video conferencing

When children are unable to attend school for a period of time, such as during a pandemic, the school may use video conferencing to keep in touch with pupils and/or enable pupils to keep in touch with each other. Such events require parental consent, and will follow relevant guidance for safeguarding. Children will be instructed on use, such as understanding that they may be muted to facilitate communication through turn-taking and listening, and that invitations are for them only. Two members of staff will be present at any one time throughout the session.
Advice for parents and carers for keeping children safe online during COVID-19

During the recent pandemic many of our children were studying at home, and home study may return at some point. It is important for your child/children to stay both connected and safe online during such times.

Have a conversation with your child about staying safe online

Most children have a positive experience online, accessing educational resources and entertainment and connecting with friends and family. Spending time online can be beneficial for children, particularly at the moment, but we recognise that many parents may worry about online safety.

Make use of parental controls

If you have downloaded new apps or bought new devices like web cams or tablets, remember to adjust the privacy and security settings to suit you.

There is technology to help you manage the content your children can access. The Government has encouraged Internet Service Providers to help parents easily filter content. Switch on family friendly filters to help prevent age inappropriate content being accessed on devices in your home. Parental controls put you in control of what your child can see. Internet Matters has step by step guides on how to set these up.

If you are concerned or upset about something your child has seen online, seek support from the online platform using the report function on the app or website - you can often find these in the 'help' section or 'settings' or seek support from other organisations and helpline

Talk to your child

- ***Childnet*** has guidance for parents and carers to begin a conversation about online safety
- ***Ditch the Label*** teacher resources that can be helpful for parents to discuss cyberbullying
- ***GOV.UK*** also has helpful advice.

Encourage your child to speak to you or a trusted adult if they come across content that makes them uncomfortable.

If you have concerns about specific serious harms, this guidance outlines how to protect your child from the various forms of online abuse. See also our Child Protection and Safeguarding policy.

Stay safe and healthy

If you are concerned about how long your child is using their device/devices, the government has published guidance for parents and carers on supporting children and young people's mental health and wellbeing during COVID-19.

The UK's Chief Medical Officer has also provided advice on screen time.

Here are a few of the tips to help your children strike a balance:

- **Sleep matters -** Getting enough good quality sleep is very important. Leave phones outside the bedroom when it is bedtime.
- **Sharing sensibly -** Talk about sharing photos and information online and how photos and words are sometimes manipulated. Parents and carers should never assume that children are happy for their photos to be shared. For everyone – when in doubt, don't upload!
- **Talking helps -** Talk with children about using screens and what they are watching. A change in behaviour can be a sign they are distressed – make sure they know they can always speak to you or another responsible adult if they feel uncomfortable with screen or social media use.
- **Keep moving! -** Everyone should take a break after a couple of hours sitting or lying down using a screen. It's good to get up and move about a bit. #sitlessmovemore
- **Family time together -** Screen-free meal times are a good idea – you can enjoy face-to-face

conversation, with adults giving their full attention to children.

- **Use helpful phone features -** Some devices and platforms have special features – try using these features to keep track of how much time you (and with their permission, your children) spend looking at screens or on social media.

Useful links

Organisation	Link
BBC	The BBC's Own It app helps children stop and think before they press the 'send' button.
Childnet	A tool kit to support parents and carers of any age child 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.
CTIRU	You can report terrorist content they find online through the public referral tool. More information about what to report and what happens when you make a report.
Every Mind Matters	Advice and simple tips on how to maintain your mental wellbeing if you need to stay at home during the coronavirus outbreak
Internet Matters	StaySafeStayHome online resources and advice to support families.
Let's Talk About It	Support for parents and carers to keep children safe from online radicalisation.
LGfL	Support for parents and carers to keep their children safe online, including 6 top tips to keep primary aged children safe online.
Net-aware	Support for parents and carers from NSPCC, providing a guide to social networks, apps and games.
Parent Info	Provides support and guidance for parents from leading experts and organisations.
Rise Above	Public Health England's Rise Above social marketing programme aims to help build resilience and support good mental health of young people aged 10-16.
Thinkuknow	Provides advice from the National Crime Agency (NCA) to stay safe online. To help families manage during this time, the NCA has launched #OnlineSafetyAtHome, a set of fun, engaging activities based on Thinkuknow cartoons, films, games, and advice articles.
UK Council for Internet Safety	Education for a Connected World. A framework to equip children and young people for digital life.