E-Safety Policy
St John's Primary Academy

1. Contents

2. Version control

Date	Version	Revision	Owner
19/09/17	1.0	New Policy	Future Generation Trust Policy Team
25/09/18	2.0	Policy Reviewed	Future Generation Trust Policy Team
25/09/19	3.0	Annual review of policy	Future Generation Trust Policy Team
20/11/20	4.0	Annual review of policy and addition of Appendix 4 - Remote Learning	Future Generation Trust Policy Team
28.04.22	5.0	Scheduled review and addition of section 14.3 Academy profiles	Future Generation Trust Policy Team

3. Introduction

'Online actions can have offline consequences'

Future Generation Trust is committed to ensuring all pupils become safe and responsible users of existing and new technologies.

The breadth of issues classified within online safety is considerable, but they can be categorised into three areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

By raising awareness of the risks associated with ICT, we hope to encourage pupils to access social media, the Internet and mobile phones is a safe and appropriate manner.

E-safety is a child protection issue. It should be regarded as an extension of general safeguarding and led by the whole school leadership team.

4. Aims

Future Generation Trust 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

5. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and 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 cyber-bullying 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.

6. Roles and responsibilities

6.1 The governing board

The Future Generation Trust Board has overall responsibility for monitoring this policy, reviewing it annually, and holding the headteacher to account for its implementation.

The Local Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding leads (DSL).

The governor who oversees online safety for this academy is Sean Flynn.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the trust's ICT systems and the internet (appendix 3)

6.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy through regular, up-to-date and appropriate training, and for ensuring that it is being implemented consistently throughout the academy.

6.3 The designated safeguarding lead

Details of the academy's designated safeguarding lead (DSL) and deputies are set out in our **Child Protection and Safeguarding Policy.**

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy
- Working with senior leaders, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) 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 academy behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in the academy to the headteacher and/or governing board
- Ensuring e-safety is considered in the academy's approach to remote learning

This list is not intended to be exhaustive.

6.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, 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 trust'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 trust's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy behaviour policy

This list is not intended to be exhaustive.

6.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Having an awareness of online safety issues
- Implementing this policy consistently
- Modelling good online behaviours
- Agreeing and adhering to the terms on acceptable use of the trust's ICT systems and the internet (appendix 2), and ensuring that pupils follow the trust's terms on acceptable use (appendix 1)
- 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 academy **Behaviour and Anti-Bullying Policy**

This list is not intended to be exhaustive.

6.6 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 trust's ICT systems and internet (appendix 1/2)

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

6.7 Parents

- Pupils
- Pupils are expected to:
- Adhere to this policy, the Acceptable Use Agreement and other relevant policies
- Seek help from school staff if they are concerned about something they or a peer has experienced online
- Report online safety issues in line with the procedures in this policy

6.8 Visitors and members of the community

Visitors and members of the community who use the trust'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).

7. Educating pupils about online safety

Future Generation Trust ensures that all pupils receive an age appropriate input on online-safety each year throughout our ICT curriculum. Underpinning the ICT curriculum are the SMART rules, which are reinforced in school across the curriculum:

- **Safe** – encourages young people to be safe by not giving out their personal details online
- **Meeting** – draws attention to the risks associated with meeting someone you only know online
- **Accept** – highlights the risks of accepting emails, pictures and text messages from unknown sources
- **Reliable** – is a reminder that not all information found online is necessarily reliable
- **Tell** – encourages children to tell someone if something happens or they meet someone online that makes them feel uncomfortable, or if they or someone they know is being bullied online

Online-safety understanding is provided in the following ways:

- A planned online-safety curriculum is provided as part of Computing/PSHE and is regularly revisited
- The safe use of social media and the internet will also be covered in other subjects where relevant
- The academy will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this
- Pupils are encouraged to check authenticity and validate online content
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- If a staff member is concerned about anything pupils raised during online safety lessons and activities, they will follow the reporting procedure as outlined in the trust's **Child Protection and Safeguarding Policy**

8. Educating parents about online safety

We will raise parents' awareness of online safety through:

- Regular inclusion of material in newsletters
- Annual parents' online-safety meetings
- Information on academy websites
- Involvement in high profile events such as Safer Internet Day
- Providing copies of pupils' Acceptable User Agreements

This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

9. Cyber-bullying

9.1 Definition

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 academy behaviour policy.)

9.2 Preventing and addressing cyber-bullying

Complaints of online bullying are dealt with in accordance with the Trust's Behaviour and Anti-Bullying Policy. Complaints related to child protection are dealt with in line with the Trust's Child Protection & safeguarding 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 academy 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 pupils, 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 academy will also share information on cyber-bullying with 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 academy will follow the processes set out in the academy behaviour policy. Cyberbullying (along with other forms of bullying) will NOT be tolerated. All incidents of cyberbullying reported to the academy will be recorded on the academy's CPOMS safeguarding system.

Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours 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.

9.3 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, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

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 academy complaints procedure.

10. Photographic images

We educate pupils about the risks associated with the taking and sharing of images, in particular, the risks attached to publishing their own images on the internet e.g. on social networking sites.

The headteacher will inform parent(s)/carers(s) and others present at school events that photographs/videos may be taken on the basis that they are for their personal use / private retention and not for publication in any manner.

This code of conduct specifies the manner in which St John's Primary Academy will use and make available photographic images of pupils.

The academy will:

- Not use photographs in any form of internal or external publication where school does not have permission from parents to do so
- Not use photographs of pupils in swimwear
- Not reveal within the image personal details, such as full pupils' names, date of birth, home address or telephone number
- Not use any photographs of individual children either on its web site or Twitter account
- Not use photographs when children are wearing their night attire on school visits
- Images taken on iPads for EY learning journeys are only to be taken in indoor classrooms and the outdoor areas (i.e. where another staff member is in the vicinity).
- It is acceptable for staff to use mobile phones to upload messages to Twitter, relating to school activities. Staff must then remove the images as soon as the message is live

11. Acceptable use of the internet in school

All pupils, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the trust's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the trust's terms on acceptable use if relevant.

Use of the academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

12. Pupils using mobile devices in school

It may be necessary for a child to have a mobile phone in school. If this is the case, it must be switched off.

In the rare cases in which it is appropriate to have a phone in school pupils should hand this to their teacher who will organise secure storage.

If an accusation is made that a pupil has shown other pupils 'inappropriate material' then the phone should be confiscated, switched off and the SIM card removed. These will be kept in a locked drawer and the matter will be investigated by the headteacher or another member of the leadership team.

Sexting is described as 'youth produced sexual imagery' by children under the age of 18. Pupils will be encouraged to report all incidents of sexting. Teaching staff will inform the DSL who will act according to the Safeguarding policy and the guidance outlined in 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

13. Staff using mobile phones

Personal phones should be kept out of sight of pupils and on a silent setting. Mobile phones can be used in class **ONLY** to send Twitter messages.

Texting and phone calls during lesson time and play duties are for emergencies only and staff should inform the headteacher or a member of the leadership team of this necessity.

All other contact during the school day should be made through the office.

14. Social Media

When accessing and using social media for either professional or personal use, staff must ensure that they conduct themselves in a way which reflects positively on the academy.

14.1 Professional Use – School Twitter Account

Future Generation Trust is committed to the use of social networking sites for educational purposes and this is reflected by the number of users who follow the academy on Twitter.

Staff are authorised to post messages / images (in accordance with our Photographic Images Code of Practice) on the academy's Twitter account in order to communicate general information to parents / carers and promote its educational activities. The protection of pupils, the school and the individual when publishing any material online is paramount.

These communications may only take place on official (monitored) trust systems. Personal email addresses, text messaging or social media must not be used for these communications.

Notice and Take-Down Policy - Should it come to the academy's attention that there is a resource which has been inadvertently uploaded, and is inappropriate, or the academy does not have copyright permission to use that resource, it will be removed within one working day.

Any digital communication between staff and parents / carers must be professional in tone and content.

14.2 Personal Use

It is important to note that once a comment is posted on social media, it ceases to be private.

The expression of opinion on web blogs, social networks or similar sites could inadvertently reveal information which is not suitable for public consumption and staff should be mindful of this and ensure they do not engage in inappropriate behaviour.

It is expected that staff do not make academy related comments or provide academy information in social media

- These include issues such as:
- Personal opinions about the academy
- Personal discussions about colleagues
- Information or opinions of parents / pupils
- Do not accept 'friend/follow' requests from a parent / pupil or former pupil of school age
- Do ensure privacy settings are appropriately used and checked regularly
- Do not access social media during work time, other than the academy Twitter account

By following this code, the wide variety of potential issues that some professionals have encountered will be avoided.

- Remove yourself if you have previously accepted a friend request from a pupil or their family members, who you only know through professional work.
- Other users could post a photo on their profile in which you are named, so think about any photos you appear in. On Facebook, you can 'untag' yourself from a photo.
- If you do find inappropriate references and/or images of yourself posted by a 'friend' online, you are advised to contact them and the site to have the material removed.
- Any adverse, abusive, threatening or defamatory comments must be reported to the Headteacher who will follow Local Authority and Staffordshire Police guidelines given below:

"If any parent does post malicious comments about the school or staff, the first port of call would be to talk to the parent and explain why it's inappropriate; that it is harassment which is causing alarm and distress. Police advice is to put this in writing following the meeting with the parent. If it persists they can be banned from the school grounds and the police will be contacted as they are continuing to commit an offence according to section 5, 4 and 4a of the Public Order Act."

14.3 Academy Profiles

- Staff must not set up profiles on social media for academy use. Instead, a request for this must be placed with the Learning Technologies Manager or the Headteacher.
- Passwords for academy profiles can only be changed by the Giles Thatcher, Learning Technologies Manager and are given to nominated members of the academy.
- Passwords must be kept safe and not written down. Any compromise of password, suspected or otherwise must be reported to Giles Thatcher, Learning Technologies Manager immediately.
- Staff must not post items that would bring the academy's reputation into disrepute

15. How the academy 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 the behaviour policy. 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 staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

16. 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 and deputies 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.

17. Radicalisation and Extremism

Future Generation Trust ensures that pupils are safe from terrorist and extremist material when accessing the internet in school. This includes establishing appropriate levels of filtering. If a concern arises pupils will know who to go to and adults should inform the DSL and deputies who will act according to the safeguarding Policy and the guidance outlined in the Prevent and Channel Duty Guidance. The curriculum will ensure that pupils are prepared positively for life in Modern Britain.

18. Links with other policies

This policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour and Anti-Bullying Policy
- Staff Discipline Policy
- Data Protection Policy and privacy notices
- Complaints Policy and Procedure
- Staff Code of Conduct

19. Monitoring and Review

The Future Generation Trust Board has overall responsibility for this policy and for reviewing its implementation and effectiveness. The Headteacher has operational responsibility for implementation at their academy. The DSL for each academy logs behaviour and safeguarding issues related to online safety.

This policy and all arrangements for e-safety will be reviewed annually.

Policy adopted on:	5 May 2022		
Review Date:	May 2025		
Signed:	Fliss Dale	**Designation:**	Chair of the Trust Board

Appendix1: acceptable use agreement (younger pupils – EYFS/KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / Ipads.
- I will only use websites that my teacher has chosen.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.

Signed *(child)*:……

Appendix 2: acceptable use agreement (older pupils – KS2)

- I will only access computers with my login.

Safe

- I will tell my teacher about any unpleasant material or messages I find or are shown to me
- I will not give out my own details such as my name, phone number or home address
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will make sure that all ICT contacts with other children and adults are responsible, polite and sensible

Send

- I will not send to children or adults anything that could be considered unpleasant or nasty

Save

- I will not save anything that could be considered unpleasant or nasty

Search

- I will ask permission from a teacher before using the Internet

Signed (child):……

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher/IT Manager.

- I will only use the academy's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Local Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the academy or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any academy business.
- I will ensure that personal data (such as data held on Scholarpack/Schoolmoney) is kept secure and issued appropriately, whether in school or accessed remotely.
- I will not take any personal data off-site without first seeking authorisation from the Headteacher/IT Manager.
- I will not create any accounts on behalf of the academy on social media platforms including the creation of pages, groups whether public or private.
- When leaving my work-station I will always lock the screen (win key & L).
- I will not browse, download, upload or distribute material that could be considered offensive, illegal or discriminatory.
- Images of pupils will only be taken and used for professional purposes in line with the trust's **Data Protection Policy** and will not be distributed outside the academy network without consent of the parent/ carer.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.
- I will respect copyright and intellectual property rights.
- I will support and promote the trust's **E-Safety Policy** and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I agree to follow this code of conduct and to support the safe use of ICT throughout the academy.

Staff Signature ..... Date .....

Print Name .....

Appendix 4 Remote Learning

At our academy we understand the need to continually deliver high quality education, including during periods of remote learning. We recognise the importance of maintaining high expectations in all areas of school life and ensuring that all pupils have access to the learning resources and support they need to succeed.

When remote learning is necessary we will aim to

- Minimise the disruption to pupils' education and the delivery of the curriculum.
- Ensure provision is in place so that all pupils have access to high quality learning resources.
- Protect pupils from the risks associated with using devices connected to the internet.
- Ensure staff, parent, and pupil data remains secure and is not lost or misused.
- Ensure robust safeguarding measures continue to be in effect during the period of remote learning.
- Ensure all pupils have the provision they need to complete their work to the best of their ability, and to remain happy, healthy, and supported during periods of remote learning.

Where live video connections are made all staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are not permitted.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background 'private' living areas within the home, such as bedrooms, are not permitted.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

Where remote learning is in operation the academy will maintain regular contact with parents to

- Reinforce the importance of children keeping safe online
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.