CRIGGLESTONE ST. JAMES CE PRIMARY ACADEMY

Ready For The Future

E-Safety Policy

2021-22

Contents

E-SAFETY POLICY
'Ready for the Future'

Brief Rationale

Our vision, and all policies, capture our vision to see our children socially, morally and academically ready for the future. All in equal measure but driven by the social and moral aspects. We believe knowledge is nothing without knowing how, and being able to, use it to the benefit of all others. We believe that the Bible offers a message of how we can use our knowledge, skills and qualities to serve and help all others. We carry this forward each day. Our vision is rooted within this. Our school is built upon this.

St James Primary Academy is committed to valuing diversity and to equality of opportunity. We aim to create and promote an environment in which pupils, parents/carers and staff are treated fairly and with respect, and feel able to contribute to the best of their abilities. We recognise that it is unlawful to take into account anyone's gender, marital status, colour, race, nationality, ethnic or national origin, disability, religious beliefs, age or sexual orientation.

****

1. Aims

Everyone at St James is committed to ensuring that children stay safe when using technology, both in school and at home. The internet is an essential part of current education, as well as expectations regarding remote learning and is vital for children to be able to access life in the 21st century. As a school, we have the responsibility to provide the children with opportunities and skills to use quality internet access and equipment, as well as ensuring their safety using it.

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.

2. Legislation and guidance

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
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE'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.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 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 governors who oversees online safety are Kevin Morris (safeguarding) and Clair Watkins (safeguarding).

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 (appendix 3).

3.2 The headteacher

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

3.3 The designated safeguarding lead

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

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

- Supporting the headteacher (if they are not the DLS) and SLT in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher (if they are not the DSL) and SLT, IT service provider and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety or cyber-bullying incidents are recorded school system (on shared) or Safeguard Software (depending on the incident), so the behaviour lead and Safeguard Team are notified and the incident is dealt with appropriately in line with this policy.
- Updating and delivering staff training on online safety (appendix 4 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 school to the governing board.

This list is not intended to be exhaustive.

3.4 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 (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2).
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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.

This list is not intended to be exhaustive.

3.5 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 (appendices 1 and 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
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

Information regarding e-safety is available for parents on the school website.

3.6 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).

3.7 Managing IT

The IT service provider 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 school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents and cyber bullying are reported to school, who will deal with the incident appropriately in line with this policy.

This list is not intended to be exhaustive.

Monitoring and managing the children's internet safety:

Physical safety:
The following considerations are made when using the technology:

- All electrical equipment in the school is tested annually to ensure that it is safe to use.
- Any electrical equipment that breaks is stored in a cupboard until it can be replaced.
- Pupils are taught about the dangers of electricity as part of the science curriculum.
- Pupils are taught how to carry and use equipment properly to ensure they do not break easily.

3.8 Managing internet access:

Information system security
To make sure the schools network stays safe, we:

- Ensure the school ICT systems capacity and security are reviewed regularly by the IT service provider.
- Update Sophos (virus protection) regularly and ensure it is checked by the IT service provider.
- Discuss our security strategies with the IT service provider.
- Ensure all school laptops/computers require a log on and password to access the documents and internet.

- Do not share the access code for the school's secure network unless it is required for technical reasons, or for outside agencies that require access to the documents or sites.

E-mail

To make sure our school e-mail system remains safe and secure to exchange information, we:

- Only allow staff and children to use approved e-mail accounts on the school system.
- Tell children they must immediately tell an adult if they receive an offensive e-mail.
- Use their school email and password for school purposes only (Home school learning/homework) and do not tell anyone their password.
- Check e-mails we are sending to external organisations are written correctly and carefully.
- Only send emails from our staff accounts when it is school related.
- Zip sensitive data and information to protect the content using password protection.

School website and published content

To ensure the children and staff at the school are protected we:

- Only put the school's contact details on the website.
- Have designated people who update the website and any social media accounts linked to the school. They are also responsible for making sure children who don't have written parental permission to go on the website are not on it.

Don't put children's names on the website.

- Block/filter access to social networking sites for children.
- Will allow access to social networking sites for school staff if it is seen as a useful resource and good CPD opportunities, as long as they have signed the Acceptable Use Agreement (see appendix 3).

Managing filtering

The school works with the IT service provider to ensure the systems to protect the children are constantly reviewed and updated. If children or staff discover an unsuitable site, they must report it to a member of SLT who will contact the IT service provider and have the site blocked. If it is discovered by a child during a lesson, the children are encouraged to minimise the screen or turn the ipad over and report it to a member of staff straight away.

Managing technologies

To ensure we are keeping the children and staff safe with technology, we:

- Constantly research new technology and carry out a risk assessment before it is allowed to be used in school.
- Allow children who walk to and from school without adult supervision to bring a mobile phone to school; however, it is stored away during the school day in a safe place where no one can access it.
- Do not allow staff to send text messages, emails or messages through social media to parents for discussing the school, children, staff or any school business, unless it has been authorised by the Headteacher.
- Educate the children about the appropriate use of the current and emerging technology and what to do if they feel they are at risk.
- Use Meraki to initialise and control the school ipad, which are also filtered through ACS.
- Have the highest update available for the ipads.
- Do not allow sensitive data to be stored on the ipads and any data is removed at regular intervals. It is the responsibility of the class teacher, to remove data such as photographs that they have used in their lessons.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

The introduction of the new relationships and sex education (RSE) curriculum is compulsory from summer term 2021. Under the new requirement, **all** schools will have to teach Relationships education and health education in primary schools. This new requirement includes aspects about online safety.

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.

Pupils will be taught about e-safety (including the safe use of social media and the internet), through termly 'e-safety weeks' and half termly e-safety lessons. E-safety is also taught whenever the opportunity arises in class.

Each class will display the 'THINK SMART' rules where pupils can clearly see them. Before using laptops and ipads during lessons, pupils will be reminded of the relevant rules.

'Think Smart' Moto meaning…….Tell an adult; Hide your password; Interesting websites can be fun; Name calling is not cool; Keep your personal information safe Safe; Meeting; Accepting; Reliable; Tell). See Appendix 6

The 'SMART' rule poster will also be displayed next to other computers children use around school and on the lock screen wallpaper on each ipad.

5. 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. This policy will also be shared with parents on the school website and will be available upon request.

Online safety will also be covered during relevant information evenings and when appropriate on the weekly newsletter. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the safeguarding team.

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

6. Cyber-bullying

6.1 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 school behaviour policy).

6.2 Preventing and addressing cyber-bullying

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 classes.

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 and updates on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

Information/leaflets on cyber-bullying are available to parents on the website, 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 behaviour policy. 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.

6.3 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 and the school's COVID-19 risk assessment.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. 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 (appendices 1-3). 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 computer service provider will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Any detection of inappropriate use of the internet will be sent to a member of SLT via a screen shot and logged. The way the issue will be handled will depend on the severity of the misuse and links to the Safeguarding Policy.

Parents receive an updated handbook every year which outlines the expectations of the school. The handbook and additional information are available on the school's website. There is a 'Code of Conduct' which explains the appropriate use of the internet for children, parents and staff. This also includes the 'Malicious Communications Acts 1988' and 'Communications Act 2013', which explains that people are committing a criminal offence if they communicate any information about someone else (named or implied) that is offensive, threatening or false. This will not be tolerated by school.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

Covid-19 addendum

During the pandemic, not all children may be able to come to school, for example, if they are self-isolating, or if schools are closed to some children, like in lockdown. In this instance, the Government expects children to continue learning remotely at home. At St James, we will use Microsoft Teams as our online platform to support remote learning. All children will be able to access this with their school email address. They will not be able to access this with any other email address.

When working at home, we expect all children to:
- Follow the school's E-safety rules.
- Follow the school's behaviour policy, being kind to others, avoiding the use of bad language and not deliberately upsetting others.
- Inform their teacher/parent as soon as possible if someone else uses bad language and upsets them.
- Work in an environment with minimal distractions, where possible.
- If using a school device, parents/carers will need to sign a Device Loan Agreement before taking the device home.
- Contact class teachers through Teams or the class email address, set up by school, to submit work or to ask for help with work set. Personal email addresses should never be used.

If attending live sessions:
- Parents/carers will need to read the school's Remote Learning Agreement, explain this to their children and sign it before they can attend.
- Children will need to ensure their cameras are always turned off.
- Children will not be allowed to record any live sessions.
- Children will need to follow the expectations of the school's behaviour policy at all times.

If working online on Microsoft Teams (either at home or in the classroom), we expect all staff to:
- Adhere to the school's code of conduct, always acting responsibly and professionally.
- Be mindful of the environment that they work in, minimising any background noise/distractions as much as possible.
- Read the school's remote learning agreement, and follow this at all times.
- Use the school's behaviour policy to ensure good behaviour during any online sessions.
- For live sessions/pre-recorded sessions, be aware of what may be seen in the background. Ensure any personal photos are not displayed. Preferably, blur out the background or be in an environment where the background is plain.
- Only use Teams for live sessions with children in school.
- Do not contact children through personal email addresses. Only contact children through Teams or the class email address, set up by school, to give feedback/comments on work submitted.

If live sessions are taught, teachers must ensure settings are correct on TEAMS, so only the teacher can 'admit' pupils into the session. (See appendix 5 for instructions).

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.

- Communicating any issues with anti-virus and anti-spyware software to the school business manager.
- Keeping operating systems up to date – always install the latest updates.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3. Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT service provider.

10. 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 behaviour and ICT and internet acceptable use. 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/staff code of conduct. 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.

11. 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 in line with the PREVENT strategy.

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 safeguarding team 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.

12. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

Dear Parents,

At the start of every academic year, we like to remind children how to stay safe when using computing equipment in school and at home. Below is the 'Acceptable Use Agreement' that we talk to children in Reception and Key Stage One about.

We would like you to support us by talking to the children about the agreement and then asking them to sign the copy on the next page and return it to school. We would also like you to sign to say that you have discussed this with your child.

Please ensure that the form is signed and returned to school by insert date.

Your sincerely,

Computing and E-safety co-ordinator

Foundation Stage and Key Stage 1 (Home copy)

I understand that the school Acceptable Use Policy will help keep me safe and happy online.

- I only use the internet when an adult is with me.
- I only click on links and buttons online when I know what they do.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know the school can see what I am doing online when I use school computers and tablets and when using Tapestry (Reception only) or Microsoft TEAMs (Key Stage 1), including when I am at home.
- I always tell an adult/teacher/member of staff if something online makes me feel upset, unhappy, or worried.
- I use the THINK SMART rules to help remember online safety (see attached sheet).
- I will follow the school's home-learning agreement when using Tapestry or Microsoft TEAMs.
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online.
- I know that if I do not follow the rules, the school will follow the sanctions in the behaviour policy.
- I have read and talked about these rules with my parents/carers.

Foundation Stage and Key Stage 1 (School copy)

I understand that the school Acceptable Use Policy will help keep me safe and happy online.

- I only use the internet when an adult is with me.
- I only click on links and buttons online when I know what they do.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know the school can see what I am doing online when I use school computers and tablets and when using Microsoft TEAMs, including when I am at home.
- I always tell an adult/teacher/member of staff if something online makes me feel upset, unhappy, or worried.
- I use the THINK SMART rules to help remember online safety. (see attached sheet).
- I will follow the schools home-learning agreement when using Microsoft TEAMs.
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online.
- I know that if I do not follow the rules, the school will follow the sanctions in the behaviour policy.
- I have read and talked about these rules with my parents/carers.

Signed (child) …… Class……
Signed (parent/carer) ……

Appendix 2: KS2, acceptable use agreement (pupils and parents/carers)

Dear Parents,
At the start of every academic year, we like to remind children how to stay safe when using computing equipment in school. Below is the 'Acceptable Use Agreement' that we talk to children in Key Stage Two about.

We would like you to support us by talking to your child about the agreement and then asking them to sign the copy on the next page and return it to school. We would also like you to sign to say that you have discussed this with your child.

Please ensure that the form is signed and returned to school by insert date.

Yours sincerely,

Computing and E-safety coordinator

Key Stage 2 (Home Copy)
I understand that the school Acceptable Use Policy will help keep me safe and happy online at home and at school. I will use the THINK SMART rules to help keep me safe online.

Safe

- I will behave online the same way as I behave in the classroom.
- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are safe and appropriate, and if I have permission.
- I only talk with and open messages from people I know.
- I will only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.

Learning

- If I bring a mobile device into school it will be kept securely in the teacher's drawer/ cupboard until the end of the school day.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- I use school devices for school work unless I have permission otherwise.
- I will follow the school's home-learning agreement when using Microsoft TEAMs.

Trust

- I know that not everything or everyone online is honest or truthful.
- I will check content on other sources like other websites, books or with a trusted adult.
- I always credit the person or source that created any work, images, or text I use.

Responsible

- I keep my personal information safe and private online.
- I will keep my passwords safe and will not share them.
- I will not access or change other people's files or information.
- I will only change the settings on a device if a member of staff has allowed me to.

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that all school devices and systems are monitored to help keep me safe, including when I use them at home.
- I have read and talked about these rules with my parents/carers.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online.
- I know that if I do not follow the school rules then the school will follow the sanctions in the behaviour policy.

Tell

- If I see anything online that I should not or that makes me feel worried or upset, I will minimise the page and tell an adult straight away.
- If I am aware of anyone being unsafe with technology, I will report it to a teacher or the adult present.
- I know it is not my fault if I see or someone sends me something bad online. I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.

Key Stage 2 (School Copy)

I understand that the school Acceptable Use Policy will help keep me safe and happy online at home and at school.I will use the THINK SMART rules to help keep me safe online.

Safe

- I will behave online the same way as I behave in the classroom.
- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are safe and appropriate, and if I have permission.
- I only talk with and open messages from people I know.
- I will only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.

Learning

- If I bring a mobile device into school it will be kept securely in the teacher's drawer/ cupboard until the end of the school day.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- I use school devices for school work unless I have permission otherwise.
- I will follow the schools home-learning agreement when using Microsoft TEAMs.

Trust

- I know that not everything or everyone online is honest or truthful.
- I will check content on other sources like other websites, books or with a trusted adult.
- I always credit the person or source that created any work, images, or text I use.

Responsible

- I keep my personal information safe and private online.
- I will keep my passwords safe and will not share them.
- I will not access or change other people's files or information.
- I will only change the settings on a device if a member of staff has allowed me to.

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that all school devices and systems are monitored to help keep me safe, including when I use them at home.
- I have read and talked about these rules with my parents/carers.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online.
- I know that if I do not follow the school rules then the school will follow the sanctions in the behaviour policy.

Tell

- If I see anything online that I should not or that makes me feel worried or upset, I will minimise the page and tell an adult straight away.
- If I am aware of anyone being unsafe with technology, I will report it to a teacher or the adult present.
- I know it is not my fault if I see or someone sends me something bad online. I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.

Signed (child) …… Class……

Signed (parent/carer) ……

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

Acceptable Use Agreement- Staff, Governors and Visitors

ICT and related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This agreement is to ensure that all staff are aware of their professional responsibilities when using any form of ICT and to help keep staff, governors and visitors safe. All parties are expected to sign this policy annually, confirming their undertaking to adhere to its contents at all times. Any concerns, or need for clarification should be discussed with the business manager or Headteacher.

- I will only use the school's email, Internet, SharePoint and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords given to me by the school or other related authorities.
- I will ensure all passwords are complex i.e. contain lower and uppercase letters, numbers and special characters.
- 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 my mobile phone number or personal email address to pupils or parents.
- I will only use the approved email system for any communications with pupils, parents or for other school-related activities
- I will ensure that pupil's personal data is kept secure and is used appropriately. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher and with appropriate levels of security in place.
- I will not install any hardware or software on school equipment without prior permission.
- I will report any accidental access to inappropriate materials immediately to the business manger
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will ensure my computer is locked when left unattended.
- I will password protect any documents which contain sensitive information, in line with GDPR compliance.
- I will ensure I use OneDrive or SharePoint to store all school documents. I understand the use of memory sticks is not prohibited.
- If I email sensitive documentation, I will ensure the documents are password protected and will inform the recipient of the password separately.
- If I access school emails on any device other than those provided by school, I will ensure that device has 2 factor-authentications enabled i.e. on a mobile phone. The phone should be password protected and accessing emails should require a second password.
- I will not access SharePoint on non-school devices, unless permission has been given by the Headteacher /Governing Body.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes, in line with the data protection policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher in line with safeguarding policy.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the Headteacher should there be any concerns.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both inside and outside school, will not bring my professional role into disrepute. This includes ignoring invitations from pupils and parents to be part of any social networking profiles.
- I will support and promote the school's E-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- In line with GDPR regulations, I will report any stolen equipment to the Headteacher or business manager within 48 hours. This includes laptops, iPads and fobs, plus any unauthorised access to emails & SharePoint/OneDrive.

User Signature

I agree to follow this acceptable use policy and to support the safe use of ICT throughout the school.

Signature _____ Date _____

Full name _____ (printed)

Appendix 4

Remote learning: loan of equipment/resources agreement

1. This agreement is between:
1) Crigglestone St James CE Primary Academy and 2)
……

It governs the use and care of devices assigned to the pupil. This agreement covers the period from the date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

The school is lending the pupil the equipment for the purpose of remote learning during the lockdown period.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of loan.

2. Damage/loss
By signing this agreement, I agree to take full responsibility for the loan equipment issued to the pupil and I have read, or heard this agreement read aloud, and understand the conditions of the agreement.
I understand that I and the pupil are responsible for the equipment at all times whether on the school's property or not.

If the equipment is damaged/lost/stolen, I will immediately inform the school office, and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment. If the equipment is stolen, I will also inform the police immediately.

I agree to keep the equipment in good condition and to return it to the school at the end of lockdown, or at their request at any time during lockdown, in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

3. Unacceptable use
I am aware that the school monitors the pupil's activity on this device. I agree that my child will not carry out any activity that constitutes 'unacceptable use'.

4. Personal use
I agree that the pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

5. Return date
I will return the device in its original condition to the school office, upon being requested to do so.

6. Consent
By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

PUPIL'S FULL NAME	
PARENT'S FULL NAME	
PARENT'S SIGNATURE	

Record of loaned equipment

DETAILS OF PUPIL	
NAME	
CLASS	
YEAR GROUP	
ADDRESS	
PARENT'S TELEPHONE NUMBER	
LOAN DETAILS	
LOAN DATE	
DATE RETURNED	
EQUIPMENT DETAILS	
TYPE	
MAKE	
MODEL	
ASSET NUMBER	
EQUIPMENT CONDITION	
DETAILS OF ANY ADDITIONAL EQUIPMENT	

Appendix 5

Home School Learning Agreement

At times, home school learning will be the main way in which pupils access their education, such as during the pandemic. Not all children may be able to come to school, for example, if they are self-isolating, or if schools are closed to some children, like in lockdown. In this instance, the Government expects children to continue learning remotely at home. At St James, we will use Microsoft Teams as our online platform to support remote learning. All children will be able to access this with their school email address. They will not be able to access this with any other email address. If using a school device, parents/carers will need to sign a Device Loan Agreement before taking the device home.

Below are the rules which you should share and discuss with your child. To take part in TEAMs learning and live sessions, all rules must be agreed to and the form below signed by the pupil and a parent/ carer to show they have understood what is expected of them whilst using TEAMs.

When working at home, we expect all children to:

- Follow the school's THINK SMART e-safety rules.
- Follow the school's behaviour policy, being kind to others, avoiding the use of bad language and not deliberately upsetting others.
- Inform their teacher/parent as soon as possible if someone else uses bad language or upsets them.
- Work in an environment with minimal distractions, where possible.
- Contact class teachers through Teams, class emails or admin@stjamesacademy.co.uk, to submit work or to ask for help with work set. Personal email addresses should never be used.
- Only use the chat function to discuss school work or/ and school related tasks.

If attending live sessions:

- Children will need to ensure their cameras are always turned off.
- Children will not be allowed to record any live sessions.
- Children will need to follow the expectations of the school's behaviour policy at all times.

If rules are not adhered to, the school's behaviour and e-safety policy procedures will be put in place.

Sign _____(child) Date:_____

Sign _____(parent/ carer) Date: _____

Appendix 6 THINK SMART E-Safety Rules Poster