



St John's
Church of England
Academy

Part of the



**Durham &
Newcastle
Diocesan
Learning
Trust**

Online Safety Policy

Reviewed	February 2023
Adopted	February 2023
Review due date	February 2024

Durham and Newcastle Diocesan Learning Trust is a company limited by guarantee (company number 10847279) and exempt charity registered in England and Wales at Cuthbert House, Stonebridge, Durham, DH1 3RY

Contents

Our school aims to:.....	2
Legislation and guidance	2
Roles and responsibilities	3
Educating Pupils about Online Safety	5
Educating parents about online safety.....	6
Online Risks	6
Cyber-Bullying.....	6
Online Conduct	7
Online Grooming.....	8
Acceptable use of the internet in school	9
Pupils using mobile devices in school	9
Staff using work devices outside school	9
How the school will respond to issues of misuse.....	9
Training.....	10
Monitoring Arrangements	11
Links with other policies.....	11
APPENDIX 1 Secure transfer of data and access out of school.....	12
APPENDIX 2	13
Acceptable Use Agreement Staff/Volunteer	13
APPENDIX 3 Acceptable Use Agreement Pupil	18

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, including mobile and smart technology (which we refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

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](#)

[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](#), 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.

Roles and responsibilities

The Local Academy Council

The Local Academy Council has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The Local Academy Council will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead and the deputy designated safeguarding lead.

All Academy Councillors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

The Headteacher

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

The Designated Safeguarding Lead

Details of the school's DSL and the Deputy DSL 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:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Work with staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring 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 logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the governing body.

This list is not intended to be exhaustive.

The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept 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.
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- This list is not intended to be exhaustive.

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 and ensuring that pupils follow the school's terms on acceptable use.
- 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 school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy.
- Support the school in reinforcing the messages and enforcing rules and regulations communicated to the children as part of their online safety education.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.

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 resource sheet – [Childnet International](#)
- Healthy relationships – [Disrespect Nobody](#)

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.

Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum. 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.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).

- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

The safe use of social media, the internet and video games will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Educating parents about online safety

The school will raise parents' awareness of internet safety via the school website, our social media pages, Class Dojo, Parent Pay and through educational workshops provided by the Darlington Internet Safety Partnership. This policy will also be available on the school website. Online safety will also be covered during parents' evenings where relevant. 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.

Online Risks

The school will educate the children on how to act appropriately online. However, the internet exposes children to many risks. The following section outlines some of these risks and how the school aims to support children and families through this.

Cyber-Bullying

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.

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. Staff will discuss cyber-bullying with their class. 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. In relation to a specific incident of cyber-bullying that takes place in school, 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.

For incidents of cyber-bullying outside of school, children are advised to tell a trusted adult. Parents/carers are advised to report the incident to the police, review the app on which the incident took place, remove apps that are not age-appropriate and notify the school who will decide on the best course of action for educating the child(ren) further and/or signposting parents to appropriate agencies that can offer support.

The school reserves the right to investigate, where appropriate, incidents or impose sanctions on children if:

- The incident took place outside of school.
- The child has access to apps that are not age-appropriate.
- Sufficiently robust parental controls are not set up on the device.

Where a disclosure of online-bullying that took place outside of school is made to a member of staff, the school will notify the parent/carer and arrange a meeting to discuss the best course of action.

Online Conduct

Children may conduct themselves inappropriately online. Such behaviours include, but are not limited to:

- Using inappropriate language.
- Requesting friends who are unknown to them.
- Accepting friend requests from people who are unknown to them.
- Sending images/videos of themselves to people who are unknown to them.
- Posting images/videos of themselves that can be seen publicly.
- Unkindness.

The school will educate the children in online conduct. If a child is found to be conducting themselves inappropriately online outside of school, parents/carers are advised to review the app on which the incident took place, remove apps that are not age-appropriate and notify the school who will decide on the best course of action for educating the child(ren) further and/or signposting parents to appropriate agencies that can offer support.

The school reserves the right to investigate incidents or impose sanctions due to online conduct if:

- The incident took place outside of school.
- The child has access to apps that are not age-appropriate
- Sufficiently robust parental controls are not set up on the device.

Where staff become aware of inappropriate online conduct that took place outside of school, the school will notify the parent/carer and arrange a meeting to discuss the best course of action.

Online Grooming

Online grooming is a term used to describe people befriending children online in order to take advantage of them for sexual abuse and other forms of child abuse.

The school will educate the children in how to identify and avoid the risks of online grooming. If parents/carers become aware that their child is being, or at risk of being, groomed online outside of school, parents/carers are advised to contact the police, review the app on which the incident took place, remove apps that are not age-appropriate and notify the school who will decide on the best course of action for educating the child(ren) further and/or signposting parents to appropriate agencies that can offer support.

Where staff become aware that a child is being, or is at risk of being groomed, the school will notify the parent/carer and arrange a meeting to discuss the best course of action.

***The school will always become involved if any online behavior creates a safeguarding issue.**

A simplified version of this guidance and an overview of responsibilities can be found in [Appendix 4](#).

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
- Disrupt teaching
- 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
- Retain it as evidence (of a criminal offence or a breach of school discipline)
- Report it to the police

Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [screening, searching and confiscation](#).
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#).
- 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.

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

Pupils using mobile devices in school

Children who walk to and from school alone may bring a mobile device into school. The device must be handed into the office when they arrive and be collected before they leave.

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.
- 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.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date. Always install the latest updates.
- Staff members must not use the device in any way that would violate the school's terms of acceptable use.
- 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 Headteacher and/or ICT manager.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, 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 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.

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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages.
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
- Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up.
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.
- The DSL and Deputy DSL 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 [Safeguarding Policy](#).

Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the governing body.

Links with other policies

This online safety policy is linked to our:

- [Safeguarding policy](#)
- [Behaviour policy](#)
- Staff disciplinary procedures
- [Data protection policy](#)
- [Complaints procedure](#)

APPENDIX 1 Secure transfer of data and access out of school

St. John's CE Academy recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive/restricted/protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform.
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.

APPENDIX 2

Acceptable Use Agreement Staff/Volunteer

St. John's Church of England Academy

ACCEPTABLE USE AGREEMENT

(Staff/Volunteer)

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe Internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.
- St. John's CE Academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

St. John's CE Academy will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

This policy applies to any device in school. It applies across the whole network and includes WiFi.

The school carries out secure content inspection (SSL inspection). This means that when you access a site that uses techniques to secure the information between the website and yourself, the school can read the information and remove inappropriate content or prevent access to the material. Excluded from this inspection are sites that contain sensitive financial information, including banks and payment systems.

Your activity on the Internet can be monitored by the school, logs are kept of activity, whether on a school device or using your own device through the school Wi-Fi. These logs include who is accessing what material for how

long from which device.

The school email system is provided for educational purposes. Where required, the school has the ability to access your school email for safeguarding purposes.

Acceptable Use Policy Agreement

I understand that I must use St. John's CE Academy's ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that St John's CE Academy will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to St John's CE Academy's ICT systems (eg laptops, email etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that St John's CE Academy's ICT systems are intended only for educational use.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using St. John's CE Academy's ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the St John's CE Academy's website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat (e.g. Blogging) in school in accordance with the school's policies.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.

- I will not engage in any on-line activity that may compromise my professional responsibilities.

St. John's CE Academy has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs).
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install program of any type on a machine, or store programs on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others as outlined in the school E-Safety Policy. Where digital personal data is transferred outside the secure local network, it must be password protected. Paper based Protected and restricted data must be held in lockable storage.
- I understand that Data Protection Policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the Internet in my professional capacity or for school sanctioned personal use:

I will ensure that I have permission to use the original work of others in my own work is protected by copyright; I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of St John's CE Academy:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal

activities the involvement of the police.

St. John's Church of England Academy

ACCEPTABLE USE AGREEMENT

(Staff/Volunteer)

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name

Signed

Date

Please detach this page and return to the office.

APPENDIX 3 Acceptable Use Agreement Pupil

St. John's Church of England Academy

ACCEPTABLE USE AGREEMENT

(Pupil)

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe Internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the Internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

St. John's CE Academy will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users. This policy applies to any device in school. It applies across the whole network and includes Wi-Fi.

Your activity on the Internet is monitored by the school; logs are kept of activity, whether on a school device or using your own device through the school Wi-Fi. These logs include who is accessing what material for how long from which device. The school email system is provided for educational and business purposes, where required the school has the ability to access your school email, for safeguarding purposes and should a management requirement necessitate it.

Acceptable Use Policy Agreement

- I understand that St. John's CE Academy will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details etc)
- I will not arrange to meet anyone who I have only communicated with online.

- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand St. John's CE Academy systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.
- I will not use St. John's CE Academy systems or devices for on-line gaming, on-line gambling, Internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others; I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that St. John's CE Academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of St. John's Academy:

- I will only use my own personal devices (USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs).
- I will not install or attempt to install or store programs of any type on any school device, nor will I try to alter a device's settings.

When using the Internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the Internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that St. John's CE Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

St. John's Church of England Academy

ACCEPTABLE USE AGREEMENT

(Pupil)

This form relates to the student Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use St. John's CE Academy systems and devices (both in and out of school)
- I use my own devices in St. John's CE Academy (when allowed) e.g. USB devices, cameras etc.
- I use my own equipment out of St. John's CE Academy in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.

Name of Student (PRINT)

Year Group

Signed by Student

Signed by Parent

Date

Please hand this page to your teacher.

Appendix 4: Online Risk Guidance Simplified Cyberbullying – Parents Responsibilities

***This must be read in conjunction with SG policy and will always follow guidelines.
Run past Clennell**

If an incident of cyberbullying occurs whilst the children are in school, the school will:

1. Fully investigate the incident.
2. Place sanctions upon the perpetrator.
3. Inform all parents of those involved.
4. Inform the police if necessary.

If an incident of cyberbullying occurs outside of school, parents are advised to:

1. Review and delete any apps that are not age-appropriate.
2. Ensure parental controls are set up on the device.
3. Inform the police if you feel it is necessary.

If a disclosure of cyberbullying that took place outside of school is made to a member of staff, the school will:

1. Arrange a meeting with parent/carer to discuss this policy and the best course of action.

Inappropriate Online Conduct

If an incident of inappropriate online conduct occurs whilst the children are in school, the school will:

1. Fully investigate the incident.
2. Place sanctions upon the perpetrator.
3. Inform all parents of those involved.
4. Inform the police if necessary.

If an incident of inappropriate online conduct occurs outside of school, parents are advised to:

1. Review and delete any apps that are not age-appropriate.
2. Ensure parental controls are set up on the device.
3. Inform the police if you feel it is necessary.

If a disclosure of inappropriate online conduct that took place outside of school is made to a member of staff, the school will:

1. Arrange a meeting with parent/carer to discuss this policy and the best course of action.

Online Grooming

If a member of staff becomes aware that a child is being, or is at risk of being groomed online, the school will:

1. Notify parents/carers immediately.
2. Arrange a meeting to discuss this policy and the best course of action.

If parents/carers become aware that a child is being, or is at risk of being groomed online, they are advised to:

1. Notify the police.
2. Review and delete any apps that are not age-appropriate.
3. Ensure parental controls are set up on the device.
4. Notify the school who will decide on the best course of action for educating the child(ren) further and/or signposting parents to appropriate agencies that can offer support.