Online safety policy

November 2023

THE JO RICHARDSON
SUCCESS FOR ALL
COMMUNITY SCHOOL
ACHIEVE

Contents

Designated Safeguarding - Lead: Amy Howe

Head of Computing and ICT: - Michael Campbell

ICT Network and Systems Manager: - Daniel Trayler

As a school we understand that social media and the online world can be all consuming for a stakeholder. We have been a mobile free school for over a decade. This is because we want our students to have a rest from the intense online world while they are in school. The following policy has been written with the intention of showing the controls and measures we have in place to both protect stakeholder but to also capitalise on the benefits the online world offers.

1. Aims

Jo Richardson Community 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
  - Use social media to offer support and guidance to stakeholders who may need it in times of crisis

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, antisemitism, 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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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.
This policy also considers the requirements of DFE guidance around the digital and technology standards in schools. More information about this can be found using the link below
https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges#:~:text=An%20effective%20filtering%20system%20needs,assess%20and%20manage%20risk%20themselves

2. Roles and responsibilities

3.1 The Governing Body

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 governor who oversees online safety is Dave Botterill (Safeguarding Governor)

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring. All staff will complete the Hays online training on an annual basis.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children. Daniel Trayler (Network Manager) will provide information to the Governors to ensure they can execute this duty

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL). Daniel Trayler (Network Manager|) will oversee this and provide the requirement information.

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with Daniel Trayler (Network Manager) and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

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)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
    - Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is 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.

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

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other 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 (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 headteacher and/or governing board
    - Undertaking annual risk assessments that consider and reflect the risks children face.

- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
- Monitor the use of social media (See the Social Media policy in Appendix ????)

This list is not intended to be exhaustive.

3.4 The ICT Network and Systems Manager (Daniel Trayler)

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 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 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

Oversee the filtering and monitoring systems used in the school

This list is not intended to be exhaustive.

3.5 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
- 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.

3.6 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 school's ICT systems and internet (appendices 1 and 2)

Monitor their child's use of online platforms and social media.

Alerts the school in a timely fashion if there is anything that could put their child at risk

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
- Parent resources - https://nationalonlinesafety.com/
- Reporting online abuse to the police - CEOP

National Online Safety - https://nationalcollege.com/categories/online-safety

3.7 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).

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools In

Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns Pupils

in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet 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.

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.

Online safety will also be covered during parents' evenings and via the weekly newsletter. We promote the National online safety groups #wakeupwednesday

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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.

The school is a member of the National Online Safety organisation which provides whole school community training, resources and parent guides to effectively safeguard students online. We encourage parents and students to download the app and visit the website. https://nationalcollege.com/categories/online-safety

6. Cyber-bullying

We are very clear that this is a mobile free school. If parents choose to get their child a phone then we ask them to take responsibility for it. This includes monitoring its use, ensuring the appropriate filters and in place and that regular checks occur. There is nothing worse than thinking of a child being bullied in their own home due to open social media content.

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 1 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. Form tutors and Heads of Year will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. 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 (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to 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 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Students will also be educated about their responsibilities online. Staff will always act if they are provided with information about inappropriate use.

We have invested in the IMABI APP as another layer of protection for students https://www.imabi.com/inspire

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (as specified in our behaviour policy and our screening, searching and confiscation policy) can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are

- images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semihttps://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-peoplenudes: advice for education settings working with children and young people Any searching of pupils will be carried out in line with:
- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy

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

The schools police officer will be informed about any causes for concern. He may be called to assist with any investigation as appropriate

https://schoolleaders.thekeysupport.com/administration-and-management/record-keeping/data-protection/ai-dos-and-donts-for-data-protection/?marker=full-search-q-artifical%20intelligence%20policy-result-1

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

We recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

We will treat any use of AI to bully pupils in line with our behaviour management policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used. This is especially the case when marking work and other submitted work.

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 to 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.

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 available in Section

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Students using mobile devices in school

The school is a mobile free zone. This means students must not use their phones in the building at any point in the day. Staff are permitted to use their phone in their personal offices or the staff room. This policy is in place to safeguard all stakeholders. This includes clubs before or after school, or any other activities organised by the school. Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

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
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing 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 manager.

Staff must not use their personal devices (including mobile phones) to communicate with students under the age of 18. This is even if they have left school.

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. 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, 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 and 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.
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 up the risks
- 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 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.
The school is a member of the National Online Safety organisation is working to achieve certified school status in the 2022-2023 Academic year.

12. Monitoring arrangements

The School currently have the following Online Safety solutions in place:

- Impero Education Pro
- Webscreen filtering
- HomeProtect
- Sophos Endpoint Protection
- R;pple Browser Extension

Impero Education Pro
Software client installed on all school owned devices providing ICT Support staff with real-time monitoring, keyword detection and capture management.
Impero supplies a managed keyword policy providing appropriate monitoring compliance with KCSiE and UK Safer Internet Centre (more info can be found here)
When keywords are triggered, a screenshot is taken of the device (including logged in user, date and timestamp) which is then sent to ICT Support via email for review.

Webscreen filtering
Internet filter provided/managed by our Internet Service Provider (ISP) LGfL (London Grid for Learning).
Webscreen is hosted by LGfL so all incoming/outgoing traffic is subject to the filter and firewall.
ICT Support staff have access to block and/or allow websites and have the ability to run reports on activity through the filter system.

HomeProtect
Software client (provided by our ISP) that enforces the same web filtering on school owned devices that are loaned out to staff and students.

Sophos Endpoint Protection
AntiVirus software that is installed on all school owned devices. As well as protecting devices from attacks, also provides web protection powered by threat intelligence from SophosLabs and real-time intelligence from the Sophos Managed Detection and Response (MDR) team.

R;pple Browser Extension
Browser extension installed across all school devices that “discretely intercepts harmful searches maintaining user privacy and signposts to free, 24/7 mental health support”.

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.
This policy will be reviewed every year by the Assistant Headteacher responsible for online safety. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. 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
- Screen and search policy
- Restraint policy
- Cyber security policy

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

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Acceptable Use Policy Staff / Volunteers

Last Review/Amendment: 20th April 2022

As a member of staff / volunteer at JRCS / Castle Green I agree that: **General**

- I will not allow unauthorised individuals to access my network account / email / internet / intranet or other school / LA systems.
- If I believe that someone else has discovered my password or gained access, then I will change my password immediately and inform ICT Support. • I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Headteacher.
- I will report all network security concerns immediately to ICT Support.
- I will lock my workstation when I leave it unattended.

Equipment

- I will report all broken equipment on the ICT Support Helpdesk and not attempt to fix the hardware myself.
- I will not purchase and install any hardware or software without consulting ICT Support.
- I will not move any equipment without the permission of ICT Support.
- I agree and accept that any laptop loaned to me by the school is provided solely for school business or to support my professional responsibilities.

Storage & Data

- I will ensure any confidential data (see Data Protection Policy) that I wish to transport from the secure local network to another location is protected by encryption.
- All resources that are produced and used within school are owned by JRCS and cannot be transferred, copied or sold to other schools / third parties.
- I will not alter any data or resources belonging to another user without their permission.
- Using online storage such as Google Drive or Dropbox to store confidential data or school resources is not permitted. One Drive is available to all users on Office 365.
- I understand that all data on the school network can be accessed by the Headteacher and Network Manager. Members of ICT Support can also access all data apart from restricted folders.

Communications (Email and Microsoft Teams)

- I will only use the school email system and Teams conversations for any school business.
- Under no circumstances should staff contact students, parents or conduct any school business using their personal email addresses.
- All non-school devices, e.g., smartphone or tablet on which you access your school email via any app, must have a PIN or be password protected.
- Subscribing to any form of newsletter or vouchers that is not related to school business, e.g., Wowcher or Groupon, is forbidden.
- School email is not to be used for personal advertising.
- I understand that all emails and Teams conversations that are sent and received are logged and can be accessed by the Headteacher and Network Manager.

Internet (including personal devices connected to the Wi-Fi)

- I will not browse, download or send material that could be considered offensive.
- I will not download any software or resources from the internet that can compromise the network's security, or are not adequately licensed.
- The use of any social networking site between staff and students is forbidden.
- The use of any social networking should only be used for school business.
- The use of online video streaming services such as BBC iPlayer or Netflix can only be used in accordance with their T&Cs. Streaming services that are only available for personal use cannot be used within school.
- I understand that all internet and network usage is logged and can be accessed by the Headteacher and Network Manager.

Staff Remote Access

- Remote connections using the Staff Remote Access from a personal device is considered a direct connection to the school's network. It should be treated the same as if you were sitting at a workstation in school.

- Remote connections must only be established from devices that are secure and have up to date antivirus software installed.

Personal Devices

- I will not connect any laptop (or similar device) to the school network / internet that does not have up to date antivirus software.
- I will only download Microsoft Office from my school's Office 365 account for personal use and not to distribute.
- I will not use personal digital cameras or camera phones for taking or transferring images of students or staff without permission.

Mobile phones

I will reflect the school's rules on no mobile phones
I will not use my mobile phone during a lesson
I will not communicate with students or ex-students under the age of 18
I will uphold the ethos of the school and professional standards if I post any information on social media

I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action.

Signature …… Staff Code: …… Date: ……

A copy of this policy is also available in the Staff Handbook and Policies folder.
Last Review/Amendment: 20th April 2022
As a student of Jo Richardson Community School, I agree that: **General**

- I will not allow any other person to access any of my school accounts. This includes my school network account, my school Office 365 account and any other online accounts created by the school.
- If I believe that someone else has discovered my password or gained access, then I will change my password immediately and inform a member of staff.
- I will not attempt to use the school's network to access another person's account, service or computer without authorisation.
- I will only use the school's IT equipment for school use.

Equipment

- I will use the IT equipment as expected and not mistreat or attempt to cause damage.
- I will report all IT broken equipment to a member of staff and not attempt to fix it myself.

Storage & Data

- My school's personal My Documents and OneDrive should only be used to store schoolwork.
- I must not attempt to upload any malicious files or software onto the school network or Office 365.
- I understand that all data on a student's account on the school network can be accessed by staff.

Communications (Email and Microsoft Teams)

- I will only use the school's communication systems for any school business.
- I will not use my email account or Teams conversations to insult, tease or bully others.
- I will not use my email account or Teams conversations to share inappropriate images or files.
- Subscribing to any form of newsletter or vouchers that is not related to school business, e.g., Wowcher or Groupon, using my school email account is forbidden.
- I understand that all communications that are sent and received are logged and can be accessed by authorised staff.

Internet (including personal devices connected to the Wi-Fi)

- I will not browse, download or send material that could be considered offensive.
- I will not download any software or resources from the internet that can compromise the network's security, or are not adequately licensed.
- The use of any social networking site between staff and students is forbidden.
- Social networking should only be used for school business.
- The use of online video streaming services such as BBC iPlayer or Netflix can only be used in accordance with their terms and conditions. Streaming services that are only available for personal use cannot be used within school.
- I understand that all internet and network usage is logged and can be accessed by staff.
- Any personal online will uphold the teacher standards and the ethos of the school

Personal Devices

- I will not connect any laptop / tablet (or similar device) to the school network / internet that does not have up-to-date anti-virus software.

I understand that failure to comply with the Acceptable Use Policy could lead to a detention or suspension.

Appendix 6 Filtering and controls
Please refer to section 12

Appendix 7 – Social media policy

For more information about response to Social Media, please see our Social Media policy