



'Five Rivers is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment'

Internet Safety, Policy and Procedure

Five Rivers Child Care Ltd

Policy Owner	Headteacher
Authoriser	Head of Education
Date of Original Issue	01/09/2022
Date of Last Review	01/09/2026
Date of Next Review	01/09/2027
Version	V4

© Five Rivers Child Care Limited 2019, All Rights Reserved.

The content of this policy is protected by the copyright laws of England and Wales and by international laws and conventions. No content from this policy may be copied, reproduced or revised without the prior written consent of Five Rivers Child Care Limited. Copies of content may be saved and/or printed for use in relation to the business and affairs of the Company only.

Contents

1. Policy	3
1.1 Policy Statement	3
1.2 Terms and Definitions	3
1.3 Data Protection	3
1.4 Disclosure of Information	4
2. Introduction and Aims	4
3. Relevant Legislation and Guidance	4
3.1 Online Safety Act 2023	5
3.2 Definitions	5
3.3 Unacceptable Use	6
3.4 Additional Online Safety Act considerations	6
4. Staff	7
4.1 Access to ICT Facilities	7
5. Online Safety and the Online Safety Act	8
6. Monitoring and Review (Revised)	8
Appendix 1: Facebook cheat sheet for staff	8
10 rules for school staff on Facebook	8
Check your privacy settings	9
What to do if	9
A parent/carer adds you on social media	10
You're being harassed on social media, or somebody is spreading something offensive about you	10
Appendix 2: Acceptable use of the internet: agreement for parents and carers	11
Appendix 3: Acceptable use agreement for older pupils	12
Appendix 4: Acceptable use agreement for younger pupils	14
Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors	16
Appendix 6: Glossary of cyber security terminology	17

1. Policy

1.1 Policy Statement

This policy applies to all members of our school community, including staff, pupils, carers, parents, volunteers' visitors and all school users who have access to and are users of the school system ICT systems both in and out of school.

Our School will deal with such incidents within this policy and associated behaviour and preventing bullying policies and will, where known inform parents, carers and placing authorities of inappropriate e-safety behaviour that takes place out of school.

Adapted using the South West Grid for learning and the ThinkuKnow programme from CEOPS. This policy should also be read in conjunction with our Safeguarding and Anti-bullying policies

1.2 Terms and Definitions

The below table sets out a number of terms and definitions used within this document:

Term	Definition
Nil	

1.3 Data Protection

The Five Rivers Group supports the objectives of the United Kingdom General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) and other legislation relating to Data Processing, including the Human Rights Act 1998, the Safeguarding of Vulnerable Groups Act 2006 and the regulations that underpin our services. The Five Rivers Group has a statutory obligation to process personal data in accordance with the provisions of the United Kingdom General Data Protection Regulation (UKGDPR) and the Data Protection Act 2018.

Every member of The Five Rivers Group has an obligation to ensure that the information they process (use) is collected, maintained and disclosed in accordance with the United Kingdom General Data Protection Regulation (UKGDPR), the Data Protection Act 2018, the Five Rivers Group Data Protection Policy and The Five Rivers Group Data Retention Policy.

1.4 Disclosure of Information

It is a criminal offence for a person to knowingly or recklessly sell, disclose or retain personal information outside of the Five Rivers Group under section 170 DPA 2018 without a legitimate purpose and legal basis. The Five Rivers Group considers these actions unauthorised and will take all necessary action to ensure personal data is not disclosed, retained or sold without a valid legal reason including referral to the criminal investigations team of the information commissioner's office (CRIT ICO).

2. Introduction and Aims

Information and communications technology (ICT) is integral to the operation of the school and serves as a critical resource for pupils, staff (including senior leadership), volunteers and visitors. It supports teaching and learning, alongside the pastoral and administrative functions of the school.

However, ICT systems also present potential risks relating to safeguarding, data protection and online safety. These risks are increasing due to the rapidly evolving digital landscape, including social media, online gaming and artificial intelligence (AI).

Five Rivers recognises its responsibilities under the **Online Safety Act 2023**, which strengthens protections for children by placing legal duties on online platforms to reduce exposure to harmful and age-inappropriate content and improve reporting mechanisms.

This policy aims to:

- Set clear guidelines for the use of school ICT resources
- Establish expectations for safe, respectful and responsible online behaviour
- Support safeguarding responsibilities, including those influenced by the Online Safety Act
- Prevent disruption or harm caused by misuse of ICT systems
- Ensure pupils develop the skills to safely navigate online environments, including understanding risks such as harmful content, misinformation and AI-generated material
- Support pupils in understanding their rights, responsibilities and how to report concerns when using online platforms

3. Relevant Legislation and Guidance

This policy complies with the following legislation and statutory guidance:

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)

- Computer Misuse Act 1990
- Human Rights Act 1998
- Online Safety Act 2023
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education (latest version)
- Searching, Screening and Confiscation (DfE)
- National Cyber Security Centre guidance
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety guidance
- Meeting Digital and Technology Standards in Schools

3.1 Online Safety Act 2023

The Online Safety Act introduces duties on online platforms to:

- Prevent children from accessing harmful content
- Remove illegal content
- Provide accessible and effective reporting systems

In response, the school will:

- Educate pupils about online harms, platform safety features and reporting mechanisms
- Respond effectively to incidents involving external digital platforms
- Maintain up-to-date safeguarding procedures in line with evolving online risks

3.2 Definitions

- **ICT facilities:** All systems, services and infrastructure including network systems, devices (e.g. computers, tablets, phones), software, applications, websites and future technologies provided by the school
- **Users:** Anyone authorised to use school ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** Any use not directly related to employment, education or authorised school activity
- **Authorised personnel:** IT staff or managed service providers authorised to administer or monitor ICT systems
- **Materials:** Any digital content created or stored using school ICT systems (e.g. documents, images, audio, video, web content)

3.3 Unacceptable Use

The following behaviours are considered unacceptable when using the school's ICT facilities:

- Breaching copyright or intellectual property rights
- Bullying, harassment or promoting discrimination
- Breaching school policies or procedures
- Engaging in illegal activity or promoting unlawful behaviour
- Accessing or engaging in gambling, scams, phishing or financial fraud
- Accessing, creating or sharing harmful, offensive or inappropriate content
- Sharing nude or semi-nude images (consensual or non-consensual)
- Defaming the school or damaging its reputation
- Sharing confidential school or personal information
- Connecting unauthorised devices to the network
- Installing unauthorised software or interfering with systems
- Attempting to access restricted systems or data
- Enabling unauthorised access for others
- Causing damage to ICT systems
- Deleting or removing equipment or data without permission
- Causing a data breach
- Using offensive or inappropriate language
- Promoting private business unrelated to the school
- Attempting to bypass filtering or monitoring systems
- Engaging in extremist, racist, discriminatory or harmful conduct

3.4 Additional Online Safety Act considerations

- Accessing harmful content (e.g. self-harm, suicide or other high-risk material)
- Circumventing age-verification or safety controls (e.g. via VPNs or false identities)
- Creating or distributing misleading or harmful content, including AI-generated or deepfake material
- Failing to report harmful or illegal content encountered through school systems

This list is not exhaustive. The Headteacher and senior leaders will use professional judgement to determine unacceptable use.

Breaches may result in disciplinary action in line with school policy.

Artificial Intelligence (AI)

Artificial Intelligence (AI) tools are not currently used by students within the school's digital learning environment. School internet filtering and monitoring systems are in place to restrict access to AI platforms and other online services that may be inappropriate, unsafe, or not aligned with educational objectives. These safeguards help protect students from accessing unverified content, sharing personal information, or using technologies that could compromise academic integrity. The school regularly reviews its filtering arrangements and will continue to

monitor developments in AI technology to ensure a safe and secure online environment for all users.

4. Staff

4.1 Access to ICT Facilities

The Five Rivers ICT service manages staff access to ICT systems, including devices and system permissions.

Staff are issued with individual login credentials and must not share these.

Use of Phones and Email

- Staff must use school-provided email accounts for all professional communication
- Personal email accounts must not be used for school business
- Sensitive information must be handled securely and encrypted where appropriate
- Data breaches must be reported immediately to the Headteacher and DPO
- Personal contact details must not be shared with pupils or parents
- School-issued phones must be used for all work-related communication

Personal Use

- ICT systems must not be used for personal storage
- Personal use may be subject to monitoring
- Staff must be aware that personal online activity may impact professional reputation
- Social media use must align with professional standards

Remote Access

Staff working remotely must:

- Follow the same security and safeguarding protocols
- Ensure confidentiality of school data
- Adhere to Five Rivers ICT policies

Monitoring and Filtering

The school recognises that filtering and monitoring are critical safeguarding measures and has a robust filtering and monitoring system in place (Lightspeed).

The school will:

- Monitor for risks including harmful content, exploitation, and extremism
- Regularly review system effectiveness

Staff must:

- Understand their responsibilities
- Supervise pupil use of ICT
- Respond to alerts promptly
- Report concerns to the DSL

5. Online Safety and the Online Safety Act

The school are very mindful of pupils needs and appropriately:

- **Educate pupils about:**
 - Online platform safety features
 - Reporting harmful or illegal content
 - Risks linked to social media, gaming and online communities
- **Teach:**
 - Recognition of harmful content
 - Misinformation and manipulated media
 - Online grooming and exploitation
- **Support pupils to understand:**
 - That risks still exist despite legal protections
 - Their responsibility to report concerns

6. Monitoring and Review (Revised)

This policy will be reviewed annually, or sooner in response to:

- Updates to safeguarding guidance (including KCSIE)
- Developments in the implementation of the Online Safety Act
- Emerging risks such as AI, deepfakes and new technologies

Appendix 1: Facebook cheat sheet for staff

Do not accept friend requests from pupils on social media

10 rules for school staff on Facebook

- Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead

- Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional
 - Check your privacy settings regularly
 - Be careful about tagging other staff members in images or posts
 - Don't share anything publicly that you wouldn't be happy showing your pupils
 - Don't use social media sites during school hours
 - Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
 - Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
 - Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
 - Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)
-

Check your privacy settings

Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list

Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts

The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster

Google your name to see what information about you is visible to the public

Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if ...

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture

- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent/carer adds you on social media

It is at your discretion whether to respond. Bear in mind that:

- Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
- Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers

Name of parent/carers:

Name of child:

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

Our official Facebook page

Email/text groups for parents (for school announcements and information)

Our virtual learning platform

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

Be respectful towards members of staff, and the school, at all times

Be respectful of other parents/carers and children

Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way

Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident

Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers

Signed:

Date:

Appendix 3: Acceptable use agreement for older pupils

Acceptable use of the school's ICT facilities and internet:
agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT facilities and accessing the internet in school, I will not:

Use them for a non-educational purpose

Use them without a teacher being present, or without a teacher's permission

Use them to break school rules

Access any inappropriate websites

Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)

Use chat rooms

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

Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video

Share my password with others or log in to the school's network using someone else's details

Bully other people

Use AI tools and generative chatbots (such as ChatGPT or Google Bard):

During assessments, including internal and external assessments, and coursework

To present AI-generated text or imagery as my own work

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

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 for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 4: Acceptable use agreement for younger pupils

Acceptable use of the school's ICT facilities and internet:
agreement for pupils and parents/carers

Name of pupil:

When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will not:

Use them without asking a teacher first, or without a teacher in the room with me

Use them to break school rules

Go on any inappropriate websites

Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)

Use chat rooms

Open any attachments in emails, or click any links in emails, without checking with a teacher first

Use mean or rude language when talking to other people online or in emails

Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes

Share my password with others or log in using someone else's name or password

Bully other people

Use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard, to create images or write for me, and then submit it as my own work

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

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 for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet:
agreement for staff, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, 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

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 any private business, unless that business is directly related to the school

I understand 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 6: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber-attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) [glossary](#).

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.

TERM	DEFINITION
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.

TERM	DEFINITION
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.