JFS Policies – Safeguarding and Child Protection Addendum – Network Acceptable Use Policy – January 2023

Headteacher	Chair of Governing Board
	Andrew Moss
Dr David Moody	Mr Andrew Moss

Published Date	Staff	Review Date
January 2023	Dr David Moody	January 2024

Aims and Introduction

The Internet has the potential to be a valuable educational resource, of benefit not only to students, but also to their parents and their teachers.

JFS views the effective use of the Internet and the School's ICT Network in facilitating teaching and learning as a valuable tool in furthering one of the School's key aims *"………to educate its students according to their full potential and, through its curriculum, to equip students with skills and qualifications to help them make life and career choices."*

It is the intention of JFS that all students and staff should have access to the Internet and the School's ICT Network within clearly specified guidelines (see Appendix 1 and 2). Staff and students at the School will be encouraged to make use of ICT in their work and, where necessary, training will be provided. An important part of the training will be guidance on how to evaluate web pages and where to find suitable sites. By sending your child to JFS, it is deemed that you agree to these guidelines.

The School's Policy for the use of the Internet and School Network should be read in conjunction with the Data Protection Policy. It will relate to other policies, in particular, the JFS 'Behaviour and Discipline' policy and the 'Safeguarding and Child Protection' policy.

Ensuring that the Internet Provides Effective Learning

In order that the Internet may provide a valuable learning resource, the School will ensure that:

- access is planned as an integrated aspect of the curriculum in order to enrich and extend learning activities
- students are given clear objectives for Internet use
- students using the Internet are monitored appropriately
- students are informed that checks will be made on files held on the system
- access is through a filtered service which allows JFS to designate sites considered to be inappropriate (filtering will be done by the school supplier)
- the systems to protect students are regularly reviewed by the School, PFI provider, the LA and the Internet Service Provider.

Authorisation of Access to the Internet and School Network

Internet and School Network access is a necessary part of planned lessons. It is an entitlement for students based on responsible use and will be made available subsequent to the following measures:

- Parents will be sent this policy, which will inform them that students will be provided with monitored Internet access, when it is important for their education.
- Students undertaking personal study will be required to apply for Internet access individually, by signing the form entitled *Rules for Acceptable Use of the Internet and School Network* (to be countersigned by a parent or guardian).
- A record will be maintained of all staff and students who have Internet and School Network access.

Teaching Students to Access Internet Content Safely

Students will be taught to validate information before accepting it as true - an important aspect of higher levels of subject teaching. In particular, they will be taught:

- to expect a wider range of content, both in level (through PSHCE and Computing in particular) and in audience than is found in the School's Learning Resources Centre or on television
- to observe copyright when copying materials from the Web
- that the writer of an e-mail or the author of a Web page may not be the person claimed

- to report to a teacher immediately if they encounter any material that makes them feel uncomfortable
- that the internet and communication technology more generally is an ever changing aspect of society and that this presents both numerous opportunities and also potential risks. Students will be taught about how to take advantages of the opportunities and about how to protect themselves from potential risks
- about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work
- to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information
- that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Publishing on the Web

Students will be taught to publish for a wide range of audiences (see 4.1). The Headteacher will delegate editorial responsibility to appropriate staff to ensure that content published on the web by students has the following features:

- accurate content
- a good quality of presentation
- compliance with the School's guidelines for publications.

All material must be the author's own work. It should state clearly the author's identity or status and give appropriate credits to other work referred to.

The point of contact on the website will be the School's address and telephone number. Home information or individual e-mail identities will not be published.

Online Communication

Where students use on-line communication as part of their studies, communications with persons and organisations will be managed to ensure appropriate educational use and that the good name of the School is maintained.

- Students may send e-mail to approved email addresses as part of planned lessons.
- Incoming e-mail will be regarded as public.
- E-mail messages relating to school business (e.g. arranging a work placement) must be approved before being sent.

Ensuring that Internet Access is Appropriate and Safe

The Internet is essentially an unregulated digital forum. It is therefore not possible to guarantee that particular types of material will never appear on a device which accesses the internet within the School. The School cannot accept liability for the material accessed, or any consequences thereof. However, the following actions will be taken to ensure that the risks are minimal:

- the School will monitor students' usage and take all reasonable precautions to ensure that users access only appropriate material
- a virtual learning environment will be maintained by the School and within this safe and controlled environment much of the online material approved by the School, to support students with their learning, will be stored
- filtering software will ensure that access to undesirable sites is barred, wherever possible, and

inappropriate searches are prevented. This includes making sure that children are safe from terrorist and extremist material when accessing the internet

- senior staff will ensure that occasional checks are made on files to monitor compliance with the School's Internet Policy; it will be emphasised to students that their use of the Web is not private (a record is kept of all sites visited)
- senior staff will monitor the effectiveness of Internet access strategies; access levels will be reviewed as students' Internet use expands and their ability to retrieve information develops
- staff, parents, governors and advisers will work to establish agreement that every reasonable measure is being taken the Headteacher will ensure that the policy is implemented effectively.

Maintaining the Security of the School ICT System

The School's network managers will ensure that the system has the capacity to take the increased traffic caused by Internet use and will review the security of the whole system with regard to threats to security from Internet access, and will ensure that:

- virus protection is installed and updated regularly
- security strategies will be discussed with relevant authorities.

Use of e-mail to send attachments such as system utilities is not permitted.

All users are expected to protect passwords and not share accounts. These will need to be changed regularly.

Any data held will be in accordance with the requirements of the General Data Protection Regulation as from 25 May 2018.

Handling Complaints

Responsibility for handling any incident that leads to a complaint, by either students or parents, will be given to a senior member of staff.

There may be very rare occasions when the police must be contacted. Early contact will be made with relevant parties if this situation arises.

If staff or students discover unsuitable sites, the URL (address) and content will be reported to the Internet Service Provider. Any material that the School suspects is illegal will be referred to the Police.

Improper use by students of the Internet or e-mail will be dealt with using the sanctions currently employed by JFS when responding to incidents which breach the School's Behaviour and Discipline Policy and Statement of Ethos.

Training for Use of the Internet and School Network

All staff, including teachers, supply staff, learning support assistants and support staff, will be provided with the JFS Policy for the use of the Internet and School Network, and its importance explained.

Parents' attention will be drawn to the JFS Policy for the use of the Internet and School Network in a variety of ways e.g. in newsletters, the School Prospectus and on the School's Web site.

Students will be taught proper Internet use from Year 7.

Parents are encouraged to contact the School if they wish to find out additional information or receive advice about any aspect of the use of the Internet. If the School is unable to provide the required assistance, it will be happy to put parents in contact with other organisations, which have additional expertise in this field.

Appendix 1

Acceptable Use Agreement – Student Agreement

The School has installed computers with Internet access to help your learning. These rules will keep you safe and help us be fair to everyone.

- I will only access the system with my own login and password, which I will keep secret. I will not access the internet or other networks using mobile data networks during school times.
- I will not access other people's files.
- I will use the computers *only* for school work and homework.
- I will not give out my home address or telephone number, or arrange to meet someone- remove unless my parent, guardian or teacher has given permission.
- I will report to a teacher any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other students and myself.
- I understand that the School may check my computer files and monitor the Internet sites I visit.
- I will respect the interests of other people using the Internet in the same room as me, and will not deliberately access material that will distract, disturb, or offend them.
- I will not download or store in my network user area any executable files, or any copyrighted audio or video material.
- I will not attempt to access network system files or software to which I do not have access rights.
- I will not access any material which could be deemed inappropriate by the School.
- I will not take, share or manipulate any images or video of students, teachers or other school members without their full consent.
- I will use my school email address for school related activities.

Appendix 2

Acceptable Use Agreement – Staff Agreement

The computer systems (school network and office 365) may be used by staff to enhance their professional activities including teaching, research, administration and management. The School's Policy for the use of the Internet and School Network has been drawn up to protect all parties - students, staff and the School.

The School reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

All members of the JFS Workforce, since they will need access to the School Network, should sign a copy of this statement (*Acceptable Use of the Internet and School Network*) and return it to the Headteacher.

What you can expect from the School

- reliable access to the Internet for both individual professional research and for class activities
- training in the use of the Internet and School Network
- e-mail facilities

What the School can expect from you

- be appropriate to staff professional activity; accessing of inappropriate materials such as pornographic, racist or offensive material is expressly forbidden
- be via the authorised account and password, which should not be made available to any other person
- respect copyright of materials
- not threaten the integrity of the School's ICT systems, or corrupt other systems
- not be for personal financial gain, gambling, political purposes or advertising.
- not be used to store in my network user area any executable files, or any audio or video material that is not for educational use.

When using e-mail you:

- are responsible for all e-mail sent and for contacts made that may result in e-mail being received
- only use school email accounts for school business
- must employ the same professional levels of language and content as you would use for letters or other media (e-mail can be forwarded or inadvertently be sent to the wrong person)
- must not post anonymous messages or forward chain letters and follow JFS Email guidelines

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras are brought into school at the owner's risk. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Staff will be issued with a school phone where contact with students, parents or carers is required, for instance for off-site activities.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.

Cyber security and ensuring personal data is not shared

- Only School laptops should be used to access the school network remotely.
- Do not download or save sensitive or personal data on to USB sticks or personal computers.
- All documents that contain personal data that are saved onto mobile devices or laptops must be password protected and/or encrypted.

- When sharing documents containing the personal data of staff, students or parents they must be password protected and not attached to the email but hyperlinked.

DECLARATION

I agree to adhere to all the principles outlined in this form (Acceptable Use of the Internet and School Network)

Signed: __________________________ *Name:* ______________________________ *Date:* ______________

(*Block capitals*)