


# JFS Policies – Safeguarding and Child Protection Addendum – E-Safety Policy

## January 2024

Headteacher	Chair of Governing Board
	
Dr David Moody	Mr Andrew Moss

Published Date	Staff	Review Date
January 2024	Dr David Moody	January 2025

## Aims and Introduction

This policy is addendum to the school's main 'Safeguarding and Child Protection' policy. It is designed to outline the use of technology inside and outside of school.

The internet and other digital and information technologies are powerful tools which open up new opportunities for everyone. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to, loss of or sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The sharing/distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication or contact with others, including strangers;
- Cyber-bullying including racist, sexual, homophobic, biphobic and transphobic comments;
- Access to unsuitable video and internet games;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files.

Many of these risks reflect situations in the offline world and it is essential that this e-safety policy is used in conjunction with other school policies

It is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks.

## Scope of the Policy

This policy is intended for all groups with access to and use of school ICT systems, both in and out of the school. This includes all staff, students, parents, visitors and community users.

The Education and Inspections Act 2006 also empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour as set out in the 'Behaviour and Discipline' and 'Anti-Bullying' policy. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place inside or outside of the school but are linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The KCSIE September 2022 update highlights the importance of online safety training for staff and the requirement to ensure children are taught about online safety as part of effective safeguarding practice.

## Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the

school.

### *Headteacher and Senior Leaders:*

The Headteacher has a duty of care for ensuring the e-safety of members of the school community, though the day to day responsibility for e-safety will be delegated to the Designated Safeguarding Lead along with the Director of Data Development.

The Headteacher and Designated Safeguarding Lead are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff

The Headteacher and Senior Leaders are responsible for ensuring all relevant staff, including the Designated Safeguarding Lead, receive suitable training to enable them to carry out their e-safety roles and to train other colleagues. All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and the 'Acceptable Use' policy.

The KCSIE September 2023 update highlights the importance of monitoring and filtering on the school network. The school policy ensures the following points are met:

### **Online safety**

135. It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

136. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk: content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

### **Online safety policy**

138. Online safety and the school or college's approach to it should be reflected in the child protection policy which, amongst other things, should include appropriate filtering and monitoring on school devices and school networks. Considering the 4Cs (above) will provide the basis of an effective online policy. The school or college should have a clear policy on the use of mobile and smart technology, which will also reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.

### **Filtering and monitoring**

141. Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

142. The appropriateness of any filtering and monitoring systems are a matter for individual schools and

colleges and will be informed in part, by the risk assessment required by the Prevent Duty<sup>39</sup>. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs.

Governing bodies and proprietors should review the standards and discuss with IT staff

144. Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

### **Reviewing online safety**

145. Technology, and risks and harms related to it, evolve, and change rapidly. Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face.

### *Designated Safeguarding Leads (DSL):*

- The DSL should be trained in e-Safety issues and be aware of the potential for serious child protection and safeguarding issues to arise from:
  - Sharing of personal data
  - Access to illegal/inappropriate materials
  - inappropriate on-line contact with adults / strangers
  - potential or actual incidents of grooming
  - cyber-bullying – including distribution of ‘nudes’
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- liaises with the Federation/ relevant body.
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- attends relevant meetings and committees of Governors.
- checks the school’s use of social media for professional purposes regularly to ensure compliance with the Social Media and Data Protection Policies.
- Takes an active part (along with the director of data development) in monitoring the content that students are viewing in school
- Takes an active part (along with the director of data development) in improving the filtering of content that students are viewing in school

### *School IT Support Team*

School technicians will be responsible for working with the PFI providers and leadership team to ensure that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school IT Technicians in conjunction the PFI providers will also need to ensure that there are no technical obstacles to all other relevant roles identified under this policy being effective in carrying out their e-safety responsibilities:

The IT technical support team is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required e-safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy.
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- that the use of the network, internet, remote access and email is regularly monitored in order that any misuse, attempted misuse can be reported to the Senior Leader for investigation, action or sanction.
- that monitoring software and systems are implemented and updated

#### *Teaching and Support Staff:*

Teaching and Support Staff are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices.
- they have read, understood and signed the 'Acceptable Use' Policy
- they report any suspected misuse or problem to the safeguarding team
- all digital communications with students, parents or carers should be on a professional level and only carried out using official school systems.
- e-safety issues are embedded in the Computer Science and PSHCE curriculum.
- students understand and follow the e-safety and 'Acceptable Use' policy.
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and report any issues to the behaviour or safeguarding team
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- when using online video software ensure the same school protocols are followed
- they comply with relevant GDPR and data retention policies with regard to personal data

#### *Students*

Students should be aware that the following points bind their use of school systems.

- They are responsible for using the school digital systems in accordance with the 'Acceptable Use' policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- they will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking or use of images and on cyber-bullying as set out in the 'Safeguarding and Child Protection' policies.
- Should understand the importance of adopting good e-safety practice when using digital

technologies out of school and realise that the E-Safety Policy covers their actions out of school

- Understand and apply the protocols for using online messaging/audio/ video software for online learning

### *Parents or Carers*

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parent information evenings, newsletters, letters. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line pupil records
- their children's personal devices in the school (where this is allowed)

Parents must be made aware of the sanctions for inappropriate use of IT by their child as detailed in the school's 'Behaviour and Discipline' policy.

### *Governors*

Relevant governors should take part in e-safety training and awareness sessions, with particular importance for those who are members of any committee involved in technology, e-safety, health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the National Governors Association or other relevant organisation.
- Participation in School training or information sessions for staff or parents.

### **Personal Devices**

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for personal device security that need to be reviewed prior to implementing such a policy. Use of personal devices should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the principles detailed in the General Data Protection Regulation and Data Protection Act 2018
- All users are provided with and accept the 'Acceptable Use' policy
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises. This includes both web and e-safety filtering
- All users will use their username and password and keep this safe
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the Personal Device Security policy

## 2. Responding to incidents of misuse of online services

### 2.1 Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, this should be immediately reported to the DSL/Headteacher, so that decisions can be made about further involvement of the LADO and/or police. Management of allegations against staff should be dealt with in line with KCSIE. The DSL will take a lead if the incident is in relation to a student.

### 2.2 Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- The Headteacher must be notified of and approve the investigation.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the Police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Federation or national / local organisation (as relevant).
  - Police involvement and/or action
- If content being reviewed includes images of Child Abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the Police would include:
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials

- Isolate the computer in question as best you can. Any change to its state may hinder a later Police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the Police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

### 2.3 School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. In doing so the school will follow their policies on **Staff Conduct and Allegations Against Staff**, or, if the incident is instigated by a student, the relevant **Behaviour** policy.