JFS School
The Mall, Kenton, Harrow, Middlesex HA3 9TE

JFS E-SAFETY POLICY

This policy will next be reviewed in the Autumn Term of 2020 (every 3 years)
by the Curriculum Committee - Ratified by FGB 21.01.19
To be read in conjunction with the JFS Use of the Internet and School Network Policy and the JFS Safeguarding Policy

1. BACKGROUND AND RATIONALE

1.1 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.

1.2 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.

1.3 Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. Behaviour Policy and Child Protection Policy).

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. The policy that follows explains how we do this, while also addressing wider educational issues in order to help young people and their parents to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2. SCOPE OF POLICY

2.1 This policy applies to all members of the School community who have access to and are users of school ICT systems, both in and out of school.

3. ROLES AND RESPONSIBILITIES

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

3.1 Headteacher and Senior Leadership Team (SLT)

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the School community, though responsibility for the oversight of e-safety will be delegated to the relevant staff who are likely to include the E-Safety Officer, Designated Safeguarding Lead ; SLT Line Manager for Computing; Subject Leader for Computing and the Network Manager, as appropriate;
- The Headteacher and SLT are responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable Continuing Professional Development to enable them to carry out their e-safety roles and to train other colleagues, as relevant;
- The Headteacher and SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles;
- The Headteacher and the Designated Safeguarding Lead should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

3.2 The E-Safety Officer

- leads the E-safety committee;
- takes day to day responsibility for the oversight of e-safety issues and has a leading role in establishing and reviewing the School e-safety policies and 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;
- liaises with the Local Authority, where relevant;
- liaises with school ICT technical staff, when relevant;
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- proactively seeks to monitor evidence of radicalisation online;
- reports as appropriate to SLT.

3.3 Network Manager/Technical staff

The Network Manager is responsible for ensuring:

- that the School's ICT infrastructure is secure and is not open to software based misuse or malicious attack;
- that users may only access the School's networks through a properly enforced password protection policy, in which passwords are regularly changed;
- the School's filtering policy is applied and updated on a regular basis;

- that the use of the network, remote access and email is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety Officer for investigation/action/ sanction;
- that monitoring software / systems are implemented and updated to take into account new developments, such as attempts to radicalise students online.

3.4 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 Policy on the use of the Internet and School Network;
- they report any suspected misuse or problem to the E-Safety Officer for investigation;
- digital communications with students (email / Virtual Learning Environment (VLE) / social media) should be on a professional level, in accordance with the staff code of conduct and only carried out using official school systems;
- e-safety issues are embedded in all aspects of the curriculum and other school activities.
- students understand and follow the School 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 ICT activity in lessons, extra curricular and extended school activities;
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices;
- 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.
- monitor students' ICT usage for evidence of radicalisation and where this is seen, use school procedures to report this to the Designated Safeguarding Lead.

3.5 Students

- Are responsible for using the School ICT systems in accordance with the Policy on the use of the Internet and School Network, which they will be expected their parents to sign before being given access to school systems.
- If students become aware of potential radicalisation taking place online, they should report this to a teacher.

3.6 Parents and Carers

- Will endorse (by signature) the Policy on the use of the Internet and School Network;
- Should access the School website / VLE / on-line student records in accordance with the Policy on the use of the Internet and School Network;
- If parents or carers become aware of potential radicalisation taking place online, they should report this to the School or outside agencies such as CEOP (Child Exploitation and Online Protection Centre) or the Police.

4. POLICY STATEMENTS

4.1 Students

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school;
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities; this will include how to report any online abuse including that related to race, religion, homophobic, biphobic and transphobic comments and how to feel safe to do so
- Students should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information;
- Students should be helped to understand the need for the student Audible Use Policy (AUP) and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school;
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Students will be educated as to what radicalisation online is, how to recognise when this may be taking place, and what to do about it, when they see it.

4.2 Parents

The School will seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, VLE;
- Parents evenings with a focus on E-Safety;
- Reference to the LGFL website.

4.3 Staff

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum. The following principles should be applied:

- Staff should act as good role models in their use of ICT, the internet and mobile devices.
- E-Safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.
- in lessons where internet use is pre-planned, it is best practice that 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;
- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit;
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the School temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need;
- Students should be taught in all lessons to be critically aware of the materials they access on-line and be guided to validate the accuracy of information;
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff will be trained to recognise when radicalisation might be taking place online, how to recognise when this may be taking place, and what to do about it, when they see it.

5. USE OF DIGITAL AND VIDEO IMAGES – PHOTOGRAPHIC, VIDEO

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites;

- Staff are allowed to take digital or video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes;
- Care should be taken when taking digital or video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute;
- Students must not take, use, share, publish or distribute images of others without their permission;
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

6. COMMUNICATIONS

When using communication technologies the School considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Only the School email service, therefore, should be used to communicate with others when in school, or on school systems (e.g. by remote access);
- Users need to be aware that email communications may be monitored;
- Users must immediately report, to the Designated Safeguarding Lead, the receipt of emails that make them feel uncomfortable and/or are offensive, threatening or bullying in nature. This includes bullying of a homophobic, biphobic or transphobic nature. It is strongly advised that they do not respond to any such email;
- Any digital communication between staff and students or parents (via email or the VLE, for example) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications;
- Students will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material;
- Personal information should not be posted on the School website and only official email addresses should be used to identify members of staff.

7. RESPONDING TO INCIDENTS OF MISUSE

It is hoped that all members of the School community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Examples of such misuse might include:

- child sexual abuse images;
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material;
- other criminal conduct, activity or materials.

If members of staff suspect that misuse might have taken place, it is essential that the matter is brought to the attention of the E-Safety Officer and he/she will then decide on the best way to pursue the matter. This may be through the School's Behaviour and Child Protection Policy although there may also be rare occasions when it will be necessary to seek the advice of the Police.