EMMANUEL
SCHOOLS FOUNDATION

E-Safety Policy

Last review: Oct 2021
Approved: Nov 2021
Next review: Oct 2023

Contents

Emmanuel Schools Foundation E-Safety Policy

1. Guiding Principles

Emmanuel Schools Foundation ("ESF") places a strong emphasis on the importance of each student striving to achieve their 'Personal Best'. As such, students are encouraged to show self-discipline and honourable purpose at all times, whether in a traditional classroom environment or in a PC suite. Students will need to be aware of the increased accountability placed upon them as they access a range of websites and information from the Internet. In some instances, whilst using the network, students may find that they need to be courageous and not shirk from their responsibilities to report either inappropriate information or inappropriate behaviour they come across. Students should act with the utmost integrity so that they support the high standards of safety and careful use of the network which we expect from them. In the course of their careers at ESF students may require guidance from either their peers or staff. Our expectation of the student body is that students support one another, displaying compassion for those around them at all times. It is expected that students develop a humble approach to their achievements and support those around them at all times.

The purpose of Internet use in ESF is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance ESF's management functions. As part of everyday life in society students learn how to evaluate Internet information and to take care of their own safety and security. Students also learn digital literacy skills, refine their own publishing and communications with others via the Internet as well as learn respect for copyright and intellectual property rights, and the correct use of published material.

The Internet is rapidly expanding and presents many good supportive opportunities to help students. Sadly, however, its abuse has led to cyber-crime, cyber-bullying and online grooming of children by predators. ESF is uniquely placed to protect, guide and support students in this situation; students know that they are safe whilst using a computer inside the physical protection of ESF and learn how to use the Internet safely and with confidence; students and parents are kept up-to-date with threats to e-safety; and staff respond pastorally to concerns of individuals or groups of students.

2. The Enhancement of Learning

ESF's Internet access is designed to enhance and extend education and empower learners; teaching students what constitutes acceptable Internet use and training them to use age-appropriate digital tools to support their learning is an entitlement for students. make safe and appropriate use of digital applications and undertake online activities that support the learning outcomes planned for the students' age and ability. Students are educated in the effective use of digital applications, web tools, and more wider reaching digital arenas such as media streaming and gaming. Students and staff are taught to validate the accuracy of the information and to be critically aware of the materials they read.

3. Assessing Internet Risks

ESF is aware that it is not possible to completely remove the risk that staff and students might access unsuitable materials via the ESF system due to the growing quantity of information and complexity of interlinking technologies that is the internet. ESF takes all reasonable precautions (filters to restrict access, monitoring and logging of all Internet activity, etc.) to ensure that users access only appropriate material. ESF cannot guarantee that all material accessed, or any consequences resulting from Internet use, will always be age or subject appropriate. However, by teaching students how to deal with inappropriate material and malicious content, we aim to develop the resilience of students and instruct them in what to do when breaches inevitably occur either in school or at home.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence, and breaches may be reported to the police. Methods to identify, assess and minimise risks are reviewed regularly by IT Support. Users should have regard for the Acceptable Use policy and have given their agreement before accessing Trust IT resources.

4. Data Protection

Personal data is recorded, processed, transferred and made available according to the current Data Protection Act which states that personal data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- secure and accurate
- kept no longer than is necessary
- only transferred to others with adequate protection

Staff must ensure that:

- At all times care is taken to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- Personal data is stored only on secure password protected systems and devices, ensuring that that devices and browsers are properly "logged-off" at the end of any session in which they are using personal data will ensure that this protection is maintained.
- Transfer of data is undertaken using approved ESF cloud services.
- School data is not recorded to any personal devices.

5. Incidents of concern

E-Safety incidents may have an impact on students, staff and the wider school community both on and off-site, and can have legal and disciplinary consequences. All staff have a duty of care to act on and report any e-safety concerns they may have. Teachers are the first line of defence; their observation of behaviour is essential in recognising concerns about students and in developing trust so that issues are reported to the pastoral office immediately. If a member of staff observes e-safety breaches by any colleague, this must be reported to the Principal immediately. Where possible the member of staff should use Senso and screen clipping software to document the behaviour they have witnessed. *NB: The documentation of evidence of an illegal or unsafe activity (Screenshots, recording etc) and then sharing of this evidence is not considered 'distribution'.*

All members of the ESF community will be reminded annually about safe and appropriate behaviour online, and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the ESF community. During each ESF schools' personal development curriculum, students will engage with taught content to ensure they understand how to keep themselves safe online, including how to identify and report unsafe activities.

Potential child protection or illegal issues involving technology must be referred to the Designated Safeguarding Lead. Where the issue involves ESF systems, internet access or ESF provided devices, The **DSL must Immediately report** these to the Trust Director of Digital Strategy and the COO.

6. Online Abuse

Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones. Children and young people may experience cyberbullying, grooming, sexual abuse, sexual exploitation or emotional abuse.

Online abuse can happen 24 hours a day, seven days a week, and reach a child even when he or she is alone. Abusive messages and images can be posted anonymously and distributed quickly to a very wide audience. It can be difficult and sometimes impossible to trace the source. Deleting inappropriate or harassing messages, texts and pictures is extremely difficult after they have been posted or sent.

All incidents of online abuse **must be** reported, recorded and investigated. Consequences for those involved in online abuse may include:

- the student responsible will be asked to remove any inappropriate material or a service provider may be contacted to remove content if the student refuses or is unable to delete content;
- Internet access may be suspended at the school for the user for a period of time. Parents of students will be informed;
- the police will be contacted if a criminal offence is suspected and further action by either the school or ESF will be taken accordingly. (See Appendix 1)

7. The Online Learning Environment (OLE)

ESF Systems for online learning are carefully monitored. The Digital Strategy Group annually reviews and updates the Policy regarding the use, and all users are informed of any changes made.

- Only members of the current student, parent and staff community have access to the OLE.
- All users should be mindful of copyright issues and only upload appropriate content onto the OLE.
- When staff and students leave ESF their account or rights to specific school areas are disabled.
- Any concerns about content on the OLE may be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - The material will be removed by the IT and Digital Services Team if the user does not comply.
  - Access to the OLE for the user may be suspended.
  - The user will need to discuss the issues with a member of the senior management team before reinstatement.
  - A student's parent may be informed.

8. Mobile Phones and Personal Devices Guidance for Students

The use of mobile phones and personal devices by students to support learning is encouraged within a Bring your Own Device lesson, or phase of a lesson. It is also encouraged for those students who have study periods and those who may attend after school study sessions, where the use of a device is appropriate to their learning goals.

- Electronic devices of all kinds are the responsibility of the user. ESF accepts no responsibility for the loss, theft or damage of such items. Nor will ESF accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the ESF community and any breaches will be dealt with as part of the Trusts and local schools Behaviour and Discipline Policy.
- Unless a Mobile phone and/or personal devices is being used to support learning in a lesson, They should be switched off and in a bag.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- If a student breaches the school Policy then the phone or device will be confiscated and will be held in a secure place. The phone or device may be accessed by a senior member of staff, in line with DFE guidelines on 'stop and search' and in the presence of the student, who will be expected to consent to a proportionate request. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence, the phone will be handed over to the police for further

investigation. Mobile phones and devices will be released in accordance with school Policy.

- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact their parents they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact Reception.

- Students should always protect their phone numbers and any device access protection. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

9. Personal Devices Guidance for Staff

Staff are permitted to use mobile phones and personal devices within the grounds of the school. Advances in technology have moved on considerably and many ESF employees have made a personal choice to utilise their personal device to access ESF systems such as Office 365, Bromcom and 3CX. The Digital Strategy Group supports and encourages the use of these devices, but staff should remain cognisant of the guidance below.

- Any device should have security features enabled, including, but not limited to – access passcode, biometric recognition, auto lock time and two factor authentication.
- Staff should not use their own personal phones or devices for contacting students or parents/carers within or outside of the School in a professional capacity.
- Staff should join the ESF-BYOD wi-fi when using their device in school, to ensure they have appropriate protection and security controls in place.
- Staff should be explicit with students about purpose when they are using a mobile device as part of a teaching and learning activity – this should be seen as an educational opportunity
- Senior Leadership Teams should consider informing students that new technology enables teachers use mobile devices in a professional capacity, but the expectations for students remain the same.
- Staff should not use their own personal devices for storing ESF data, when accessing ESF data via a personal device, staff should use the appropriate cloud application and authenticate access via ESF credentials.
- Staff should report the loss of any personal device that has been used to access Trust resources to the IT and Digital Services Team via a Support Desk Request such that the team can conduct an analysis to ensure that the Trust has not been exposed to additional or unacceptable risk.

10. Network users

Network users who deliberately access, or try to access, material that could be considered illegal will be referred to the Principal, to the pastoral team (in the case of students), to the Head of HR (in the case of staff) or the police depending on the severity of the incident. Access to the network and Internet may be removed. Other ESF sanctions covered in the Staff Handbook or other relevant policy documents may be implemented.

No network users should visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to illegal and unacceptable use of the network including:

- viewing, distributing or accessing (or attempting to do so) of pornography
- promoting of any kind of discrimination
- threatening behaviour, including promotion of physical violence or mental harm
- child sexual abuse images (the making, production or distribution of indecent images of children), grooming, incitement, arrangement or facilitation of sexual acts against children, possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) or any other information which may be offensive to colleagues or breaches the integrity of the ethos of ESF or brings ESF into disrepute
- using ESF systems to run a private business
- using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by ESF
- breaching copyright or revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- unfair usage (downloading/uploading large files that hinders others in their use of the Internet)

- on-line gaming (non-educational)
- on-line gambling
- use of social media, messaging apps or inappropriate use of video broadcasting, eg YouTube, outside of those needed for educational purposes
- inappropriate personal use of the Internet/social media /personal email
- unauthorised downloading or uploading of files
- allowing others to access ESF network by sharing username and passwords or attemptingto access or accessing ESF network, using another person's account

- careless use of personal data, e.g. holding or transferring data in an insecure manner
- deliberate actions to breach data protection or network security rules
- corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students
- actions which could compromise the staff member's professional standing
- actions which could bring into disrepute or breach the integrity of the ethos of ESF
- using proxy sites or other means to subvert ESF's filtering system
- accidentally accessing offensive or pornographic material and failing to report the incident
- breaching licensing regulations
- continued infringements of the above, following previous warnings or sanctions

In addition to the above, unacceptable use of the network by students includes:

- unauthorised use of non-educational sites during lessons
- unauthorised use of mobile phone/digital camera/other mobile device
- unauthorised use of social media/messaging apps/personal email
- unauthorised downloading or uploading of files
- allowing others to access ESF networks by sharing username and passwords
- attempting to access or accessing the ESF network, using another student's account or the account of a member of staff
- corrupting or destroying the data of other users
- sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- continued infringements of the above, following previous warnings or sanctions
- using proxy sites or other means to subvert ESF's filtering system
- accidentally accessing offensive or pornographic material and failing to report the incident
- receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

11. Communication

Many students are very familiar with the culture of mobile and Internet use. As students' perceptions of the risks may vary, e–safety expectations are explained in Computing lessons and also in the student and parent agreement form which includes a copy of school e–safety rules (these are superceded by the Trust equivalent document):

- All users are informed that network and Internet use will be monitored.
- An e–safety programme has been established across ESF to raise the awareness and importance of safe and responsible Internet use amongst students.
- All network users are bound by the ESF Acceptable use Policy.

To protect all staff and students, ESF implements Acceptable Use policies – The Student AUP can be located here (insert link) and the Staff Agreement here (insert link). Key online e-safety elements are noted below:

- Staff are made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, is provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use are supervised in this function by their line manager; there are clear procedures for reporting issues.
- ESF will highlight useful online tools which staff use with students in the classroom. These tools vary according to the age and ability of the students.

Our School communities attention is drawn to e–safety practice in newsletters, school prospectuses and on each schools website. A partnership approach to e-safety at home and at the school with parents is

encouraged. Parents

are requested to sign an e–safety agreement as part of a Home School Agreement. Parents are encouraged to read ESF Acceptable Use Policy for students and discuss its implications with their children.

12. Managing Information Systems

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and students.

Securing information systems access is covered by the ESF Service Level Agreement and IT and Digital Services Operational Handbook, which includes but, is not limited to:

- Use of individual accounts only.
- Timeouts.
- Password ageing.
- Password standards.
- Guest access.

Local Area Network (LAN) security issues include provision that:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For ESF staff, flouting electronic use policy is regarded as a reason for dismissal.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

ESF's broadband network is protected by a cluster of high-performance firewalls at the breakout point to the Internet. Filtering uses a proxy server.

- The security of ESF information systems and users will be reviewed regularly.
- Virus protection is updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Only authorised portable media is allowed to transport information.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on ESF's network will be regularly checked.
- The network manager reviews system capacity regularly.
- The use of user logins and passwords to access the ESF network will be enforced.
- Access to resources between sites is limited by the use of file/folder permissions.

13. Email

In ESF context (as in the business world), email should not be considered private and most schools and many firms reserve the right to monitor email. It is important that staff understand they should be using a work provided email account to communicate with parents, students and other professionals for any

official ESF business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

Email accounts should not be provided which can be used to identify both a student's full name and their school.

- Students must immediately tell a designated member of staff if they receive offensive email.
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole class or group email addresses will be used for communication outside of ESF.
- Sixth Form students must only use official ESF provided email accounts to communicate with staff, students and parents, as approved by the Senior Leadership Team.
- Email sent to external organisations must be written carefully and authorised before sending, in the same way as a letter written on ESF headed paper would be.
- The forwarding of chain messages is not permitted.

14. Published Content

The relevant Principal, in partnership with the Digital Strategy Group, takes overall editorial responsibility for online content only on their website. The Digital Strategy Group will ensure that content published for ESF is accurate and appropriate, whilst maintain oversite of all ESF web and social media presence.

15. Publication of Students' Images or Work

Images and videos of a student should not be published without written consent from those able to give it. Students will be taught the reasons for caution in publishing personal information and images online:

- Images or videos that include students are selected carefully and will not provide material that could be re-used.
- Students' full names are not to be used anywhere on the website, particularly in association with photographs.
- Students work can only be published with their permission or the parents.

Written consent is kept by ESF where students' images are used for publicity purposes, until the image is no longer in use**.**

16. Filtering

Levels of Internet access and supervision will vary according to the student's age and experience. Access profiles must be appropriate for all members of the ESF community. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily.

Access controls fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- A walled garden or "allow list" restricts access to a list of approved sites. Such lists inevitably limit students' access to a narrow range of content.
- Dynamic content filtering examines web page content or email for unsuitable words.
- Keyword lists filter search engine searches and URLs for inappropriate results and web addresses.
- URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate student access.

Filtering is not 100% effective, breaches will happen, and inappropriate content may be accessed. Students should always be supervised when using Internet access even though they have agreed to the IT Acceptable Use Agreement when logging onto a school computer. Each school will maintain an Incident Log to report breaches of filtering or inappropriate content being accessed.

Teachers should always evaluate any websites/search engines before using them with students; this includes websites shown in class as well as websites accessed directly by the students.

- ESF's broadband access includes filtering appropriate to the age and maturity of students.
- ESF works with an external provider to ensure that filtering policy is continually reviewed.
- ESF has a clear procedure for reporting breaches of filtering. All members of ESF community (all staff and all students) will be aware of this procedure.
- If staff or students discover unsuitable sites, the URL will be reported to the schools Network Manager who will then record the incident and escalate the concern as appropriate.
- ESF's filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- Changes to ESF filtering policy are managed by the Digital Strategy Group and approved by the COO.
- The Digital Strategy Group ensures that regular checks are made to ensure that the filtering methods selected are effective.

17. Video Calling and Video Conferencing

Video Conferencing is available by using Microsoft Teams which is secured by Internet policies. All foundation staff have access to video calling devices via their school laptop or fixed workstation. The use of this technology is covered in the AUP.

18. Emerging Technologies

ESF will keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety has been established