# e-Safety Policy

| | |
|---|---|
| **Policy Type:** | **Local** |
| **Approved by:** | **Principal** |
| **Effective from:** | **October 2020** |
| **Revision date:** | **October 2021** |

## Introduction

The Sixth Form College Farnborough recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all students and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use.

Our approach is to implement appropriate safeguards within the College while supporting staff and students to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard students we will do all that we can to make our students and staff stay safe online and to satisfy our wider duty of care. This e-Safety policy encompasses safeguarding, acceptable use, e-Security, anti-bullying, disciplinary, digital literacy and child protection. It should be read alongside other relevant College policies.

## Creation, Monitoring and Review

Our College e-Safety Group is made up of different stakeholders including:

- Director of Learning Technologies (e-Safety Officer)
- Director of Software Development and Communication
- Director of Networked Systems
- Assistant Principal - Pastoral (Designated Safeguarding Lead)
- Assistant Principal - Teaching, Learning and Assessment
- Human Resources Business Partner

This policy is based on a template that was amended by the Wessex Group e-Safety Working Group in October 2014. It makes full use of the JISC Legal e-Safety template and we are grateful for the work that they had already done. We have changed some terminology and edited the text to better reflect reality at the Sixth Form College Farnborough. For more information, go to the Links tab on JISC Legal's e-Safety page.

The e-Safety group reviewed this proposed policy during February 2015 after which the policy was approved by the senior leadership team and college Governors. The impact of the policy will be monitored regularly with a full review being carried out once a year. The policy will also be reconsidered where particular concerns are raised or where an e-Safety incident has been recorded.

This policy was developed in parallel with an e-Safety review conducted in autumn 2014 based on the 360° safe review tool http://www.360safe.org.uk/ which helped identify areas for improvement. These targets are listed at the end of this document.

The policy was reviewed in October 2016. The 'Investigating Allegations of Child Pornography' section was added making a separate document redundant. This policy was again reviewed in January 2017 and clarification over the use of discussion forums was added.

The policy was amended in October 2020 to reflect the changes in online interactions between staff and students arising as a result of an increase in the use of blended learning. In particular, the use of video conferencing tools for lesson delivery.

## Policy Scope

The e-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phones, social media sites and any other digital service where you are identifiable as a member of the College community. The policy applies to all members of the college community, including all enrolled students, all staff and workers, and applies at all times.

## Behaviour

The Sixth Form College Farnborough will ensure that all users of technologies adhere to the standard of behaviour as set out in the Acceptable Use Policy for staff and students.

Any user of College IT systems, both on the premises and remotely, must adhere to and digitally acknowledge the Acceptable use of Email, Internet and IT Services policy.

The College will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and students should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes.

Where conduct is found to be unacceptable, the College will deal with the matter internally. When it is considered that an offence has been committed, the College may report the matter to the appropriate authorities. This may include the Local Children's Safeguarding Board and/or the police.

## Roles and Responsibilities

All members of the College community should know their responsibilities for e-Safety. All staff are responsible for ensuring the safety of students and should report any concerns immediately to the e-Safety Officer, Child Protection Officer or other member of the child protection team as detailed in the safeguarding training that is compulsory for all staff.

When informed about an e-Safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

All personal tutors are required to deliver e-Safety lessons to classes as part of the tutorial programme. Leading on from this, all students must know what to do if they have e-Safety concerns and who to talk to. In most cases, this will be their tutor. Where any report of an e-Safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where appropriate, the child protection officer may be asked to intervene with appropriate additional support from external agencies.

### e-Safety Officer

The e-Safety Officer is responsible for keeping up to date with new technologies and their use, as well as attending relevant training. He/she will be expected to lead the e-Safety Group, complete, review and update the e-Safety Policy and facilitate staff development and training, including refreshers at the start of academic years and induction for new staff.

### Students

Students are responsible for using any IT systems and mobile devices in accordance with the College Acceptable Use Policy, which they must acknowledge at the time of registration. Students must act safely and responsibly at all times when using the internet and/or mobile technologies. They attend tutorial lessons that include e-Safety guidance and are expected to know and act in line with other relevant College policies e.g. mobile phone use, sharing images, cyber-bullying etc. They must follow reporting procedures where they are worried or concerned, or where they believe an e-Safety incident has taken place involving them or another member of the College community.

### Staff

All staff are responsible for using any IT systems and mobile devices in accordance with the College's Staff Acceptable Use Policy. Staff are responsible for attending staff training on safeguarding and displaying a model example to students at all times through embedded good practice. All digital communications with students must be professional at all times and be carried out in line with the staff code of conduct. All staff should apply relevant ollege policies and understand the incident reporting procedures.

## Risk Assessment

Before using a new online platform with students the e-Safety officer must be consulted. If appropriate, the e-Safety officer may request a brief risk assessment of the platform be carried out.

## Social Media and Discussion Forums

The use of social media sites, e.g. Twitter, is only acceptable if no private communications between staff and students is undertaken. No communication is permitted to occur without full visibility and accountability. As already mentioned, the e-Safety officer must be consulted to confirm a social media site is usable, if so, and what precautions need to be taken.

Teachers and other staff members must not add students as 'friends' on social networking sites, i.e. visibility of either party's private profiles should not be allowed. The exception to this rule is immediate family members. This is for the protection of both students and staff; failure to follow this guidance could result in disciplinary action.

Any use of publicly visible networks, e.g. Twitter must be recognised as globally visible publications with the same implications of publishing material in a newspaper, etc. Staff can be held directly accountable for posts which present the College in such a way that could be detrimental to future applicants or public perception of the College.

It is strongly recommended that profiles on services like Facebook should have their privacy settings at a sufficiently high level such that any anonymous individuals viewing these profiles are unable to view any personal information, photo albums or comments. It is strongly recommended to check these settings regularly.

Staff should not direct students to make use of private communication mechanisms as part of lesson delivery and private study. For example, requesting students use chat rooms and private forums, outside of official College platforms, is not permissible.

## Use of Images and Video

The use of images or videos is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or students.

All students and staff should understand the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted on to social networking sites.

The tutor team will provide information to students on the appropriate use of images. This includes photographs of students and staff as well as using third party images. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

Photographs of activities on the College premises should be considered carefully and have the consent of the person involved before being published. Consent for this is obtained via the Enrolment card. A list of any students who opt-out will be provided to the College marketing team for consideration when publishing photographs.

## Video Conferencing Tools and Virtual Lesson Delivery

Video Conferencing tools, e.g. Google Meet, Microsoft Teams, etc., provide a powerful mechanism for remote lesson delivery, interviews, 1-to-1 tutorials and other meetings.

The College is adopting a 'cameras on' policy, unless it is technically impossible to do so (i.e. no access to a webcam), for any interactions between staff and students on such platforms. The rationale is that it is exceedingly difficult to assess the wellbeing of students who may not be able to physically attend College if you cannot see them. Our safeguarding responsibilities require the ability to assess and confirm the wellbeing of students in difficult situations (e.g. the 2020 Covid-19 lockdown).

To protect all participants involved, the recording facility should be used in any video conference between staff and students. These recordings should be kept until the conclusion of the academic year, at which point they should be deleted.

## Security

The College will do all that it can to make sure the College network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and firewalls to prevent accidental or malicious access of College systems and information. The College reserves the right to monitor College provided email accounts.

## Personal Information

Any processing of personal information needs to be done in compliance with the Data Protection Act 2018 (GDPR) and we will process and store in accordance with the legislation. This includes content such as student records, e-portfolios and assessed work. The College is legally obliged to take steps to minimise the risk that data will be lost and processed unfairly. No personal information can be posted to the College website without the permission of a member of the senior management team, unless it is in line with our Data Protection Policy.

Staff must keep students’ personal information safe and secure at all times. When using an online platform, all personal information must be password protected. Every user of IT facilities is required to log off or lock their device on completion of any activity, or where they are physically absent from a device for any period.

## Education and Training

With the current unlimited nature of internet access, it is impossible for the College to eliminate all risks for staff and students. It is our view therefore, that the College should support staff and students stay e-safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively

### For Students

Students should have e-safety embedded into all courses using e-learning technologies. Issues associated with e-Safety apply across the curriculum and students should receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies. Students should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search.  Within classes, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

### For Staff

Staff will take part in mandatory safeguarding training, including e-Safety issues, before beginning a new college year. Guidance and further information will be issued to all staff following the session. The attendance of staff members at these sessions will be recorded. Any new or temporary users will receive training on the College IT system, led by the Director of Learning Technologies/e-Safety Officer. They will also be asked to sign the College's Staff Acceptable Use Policy.

## Incidents and Response

Where an e-Safety incident is reported to the College this matter will be dealt with very seriously. The College will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a student wishes to report an incident, they can do so to their tutor, Child Protection Officer or e-Safety Officer. Where a member of staff wishes to report an incident, they must contact the Child Protection Officer, e-Safety Officer or other member of the child protection team as soon as possible. Following any incident, the College will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. This is in line with the College Acceptable Use Policy, the Anti-Bullying Policy and the Safeguarding Policy. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

## Investigating Allegations of Child Pornography

If there is evidence of child pornography being displayed on computers at the College, or stored using a College service (locally or cloud based), the Principal must be informed immediately. If he/she is not available, the most senior Director/Assistant Principal available should be informed.  The Principal (or alternate) will contact the police immediately and hand the investigation over to them. The basic rule is simple – downloading and using images of child pornography is a criminal offence and must be investigated by the police, not by College staff. Under no circumstances may copies of material be made.