Online Safety and Acceptable Use Policy

College	**FAR Academy - Whitstable**

Policy owner:	Brent Lewis - Headteacher
Queries to be directed to:	Brent Lewis

This policy will be reviewed on an annual basis.

Date of last review:	November 2024
Date of next review:	November 2025

Contents

---

1. Aims

Our college aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Identify and support individual students that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole college community in its use of technology, including mobile and smart technology (which we refer to as ‘mobile phones’)
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

It upholds the principles of protecting vulnerable users from harmful content online, as per the Online Safety Act 2023, the new offences introduced by the Act and the categories of harmful content that platforms need to protect children from https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

This policy complies with our funding agreement.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard students.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure students are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the college has appropriate filtering and monitoring systems in place on college devices and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with the headteacher what needs to be done to support the college in meeting the standards, which include:

- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree to the terms on acceptable use of the college's ICT systems and the internet (Appendix 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-college approach to safeguarding and related policies and/or procedures

- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for especially vulnerable students. This is because of the importance of recognising that a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the college.

3.3 The designated safeguarding lead (DSL)

Details of the college's designated safeguarding lead (s) (DSL) are set out in our Safeguarding Policy.

The Headteacher is also a DSL and takes the lead responsibility for online safety in college, in particular:

- Supporting the staff to understand this policy and that it is being implemented consistently throughout the college
- Working with the DSLs and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on college devices and college networks
- Working with the staff to make sure the appropriate systems and processes are in place
- Working with the other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the college's Safeguarding Policy
- Ensuring that any online safety incidents are logged (see Appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the college policies
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in college to the DSLs and governing board
- Undertaking annual evaluation to consider and reflect the risks students face
- Providing regular Safeguarding updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

3.4 The headteacher

The headteacher is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on college devices and college networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at college, including terrorist and extremist material
- Ensuring that the college's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the college's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see Appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with college policies
- Upholding the principles of protecting vulnerable users from harmful content online, as per the Online Safety Act 2023, with clear understanding of the categories of harmful content that platforms need to protect users from

3.5 All staff and volunteers

All staff and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the college's ICT systems and the internet (Appendix 2), and ensuring that students follow the college's terms on acceptable use (Appendix 1)
- Knowing that the Headteacher is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing via the office.
- Following the correct procedures by contacting the Headteacher or office if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSLs to ensure that any online safety incidents are logged (see Appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the college policies
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'
- Upholding the principles of protecting vulnerable users from harmful content online, as per the Online Safety Act 2023, with clear understanding of the categories of harmful content that platforms need to protect users from

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of office staff or the headteacher of any concerns or queries regarding this policy
- Support their child or young person to read, understand and agree to the terms on acceptable use of the college's ICT systems and internet (Appendix 1)

Parents/carers can seek further guidance on keeping children and young people safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – https://www.childnet.com/help-and-advice/11-18-year-olds
- The Online Safety Act 2023, the new offences introduced by the Act and the categories of harmful content that platforms need to protect children from https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

3.7 Visitors

Visitors who use the college's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 2).

4. Educating students about online safety

Students will be taught about online safety

By the **end of their attendance at college**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online

- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- How the Online Safety Act 2023, introduces new offences and the categories of harmful content that platforms need to protect children from https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer
- Where necessary, teaching about safeguarding, including online safety, will be adapted for especially vulnerable students. This is because of the importance of recognising that a more personalised or contextualised approach may often be more suitable

5. Educating parents/carers about online safety

The college will raise parents/carers' awareness of internet safety in communications home, and in information via our website. This policy will also be shared with parents/carers.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of the leadership team.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Teaching staff will use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

The college also signposts information on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the college will follow the processes set out in college policies. Where illegal, inappropriate or harmful material has been spread among students, the college will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the college rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the headteacher / DSL.
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the college or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the headteacher in conjunction with the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our policies

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the college complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

The college recognises that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The college will treat any use of AI to bully students in line with our policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used.

7. Acceptable use of the internet in college

All students, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the college's ICT systems and the internet (Appendices 1 and 2). Visitors will be expected to read and agree to the college's terms on acceptable use if relevant.

Use of the college's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in Appendices 1 and 2.

8. Students using mobile devices in college

Students may bring mobile devices into college but are not permitted to use them during teaching time.

Any use of mobile devices in college by students must be in line with the acceptable use agreement (see Appendix 1).

Any breach of the acceptable use agreement by a student may result in the requirement to surrender their device at agreed times.

9. Staff using work devices outside college

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the college's terms of acceptable use, as set out in Appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the headteacher.

10. How the college will respond to issues of misuse

Where a student misuses the college's ICT systems or internet, we will follow the procedures set out in our policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the college's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The college will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required.

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children and young people are at risk of online abuse
- Children and young people can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on CPOMS. In addition, an incident report log can be found in Appendix 3.

This policy will be reviewed every year by the headteacher. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety and acceptable use policy is linked to our:

- Safeguarding policy
- Staff Code of Conduct
- Complaints procedure

Appendix 1: Acceptable Use Agreement (Students)

ACCEPTABLE USE OF THE COLLEGE'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS	
Name of student:	
I will read and follow the rules in the acceptable use agreement policy. **<u>When I use the college's ICT systems (like computers) and get onto the internet in college</u>** **I will:** • Always use the college's ICT systems and the internet responsibly and for educational purposes only • Only use them when a member of staff is present, or with a member of staff's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a member of staff immediately if I find any material that might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the college's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into college:** • I will not use it during lessons without a member of staff's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the college will monitor the websites I visit on college devices and that I will need to surrender my devices during lessons if I don't follow the acceptable use policy.**	
Signed (student):	**Date:**
For a student under 18 **Parent/carer's agreement:** I agree that my child can use the college's ICT systems and internet. I agree to the conditions set out above for students using the college's ICT systems and internet, and for using personal electronic devices in college, and will make sure my child or young person understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: Acceptable Use Agreement (Staff, Governors, Volunteers)

ACCEPTABLE USE OF THE COLLEGE'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS	
Name of staff member/governor/volunteer:	
When using the college's ICT systems and accessing the internet in college, or outside college on a work device (if applicable), **I will not:** • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way that could harm the college's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the college's network • Share my password with others or log in to the college's network using someone else's details • Take photographs of students without checking with the leadership team first • Share confidential information about the college, its students or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the college	
I will only use the college's ICT systems and access the internet in college, or outside college on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the college will monitor the websites I visit on college devices. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside college, and keep all data securely stored in accordance with this policy. I will let the designated safeguarding lead (DSL) know if a student informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the college's ICT systems and internet responsibly and ensure that students in my care do so too.	
Signed (staff member/governor/volunteer):	**Date:**

Appendix 3: Online Safety Incident Report Log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**