KITE COLLEGE
Kent Inclusive Technical Education

Online Safety Policy

Date: January 2024

Policy Reference:

Authorised Principal: Steve Badder/Sarah Miller

Review Date: January 2025

Signed:

Bob Law

Sarah Miller

Contents

1. Aims 3
The 4 key categories of risk 3
2. Legislation and guidance 3
3. Roles and responsibilities 4
3.1 The Trustee board 4
3.2 The principal 5
3.3 The designated safeguarding lead (DSL) &DDSLs 5
3.4 The ICT provider along with the DSL team is responsible for: 6
3.5 All staff and volunteers 6
3.6 Parents/carers 7
3.7 Visitors and members of the community 7
4. Educating learners about online safety 7
5. Educating parents/carers about online safety 9
6. Cyber-bullying 9
6.1 Definition 9
6.2 Preventing and addressing cyber-bullying 10
6.3 Examining electronic devices 10
6.4 Artificial intelligence (AI) 12
7. Acceptable use of the internet in college 12
8. Learners using mobile devices in college 12
9. Staff using work devices outside college 13
10. How the college will respond to issues of misuse 13
11. Training 14
12. Monitoring arrangements 15
13. Links with other policies 15

1. Aims

KITE college aims to:

- Have robust processes in place to ensure the online safety of learners, staff, volunteers and trustees
- Identify and support groups of learners 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 colleges on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for principals and college staff
- Relationships and sex education

- 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.

3. Roles and responsibilities

3.1 The Trustee board

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

The trustee 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 around filtering and monitoring.

The trustee 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 children.

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

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

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- 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 trustees will:

- Ensure they have read and understand this policy.

- Agree and adhere to the terms on acceptable use of the colleges ICT.
- Ensure that online safety is a running and am interrelated theme while devising and implementing their college approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable young people, victims of abuse and learners with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all young people in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The principal

The principal 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) &DDSLs

Details of the colleges designated safeguarding lead and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in college, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the college.
- Working with the trustee 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 ICT support provider to make sure the appropriate systems and processes are in place.
- Working with other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the colleges child & adult protection policy.
- Ensuring that any online safety incidents are logged on My Concern 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 behaviour policy.

- 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 principal and trustee board.
- Undertaking annual risk assessments that consider and reflect the risks children and young people face.
- Providing regular safeguarding and child protection 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.
- This list is not intended to be exhaustive.

3.4 The ICT provider along with the DSL team 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 learners are kept safe from potentially harmful and inappropriate content and contact online while at college, including terrorist and extremist material.
- Ensuring that the colleges 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 colleges ICT systems on a termly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are reported to the DSL team for recording on My Concern.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the college behaviour and anti-bullying policy.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency 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 colleges ICT systems and the internet and ensuring that learners follow the colleges terms on acceptable use policies and agreements.
- Knowing that the DSL team 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 by reporting via My Concern.
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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 behaviour policy.
- 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'.

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the principal of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the colleges ICT systems and internet (appendices 1 and 2).

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

3.7 Visitors and members of the community

Visitors and members of the community who use the colleges 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 3).

4. Educating learners about online safety

Learners will be taught about online safety as part of the Life Skills and Personal

- Identify a range of ways to report concerns about content and contact.

By the **end of college**, learners will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.
- 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 (including those created by 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).

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some learners with SEND.

5. Educating parents/carers about online safety

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

Online safety will also be covered during parents' evenings.

The college will let parents/carers know:

- What systems the college uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the college (if anyone) their child will be interacting with online

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

Concerns or queries about this policy can be raised with any member of staff or the principal.

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. (See also the college behaviour and Anti bullying policy.)

6.2 Preventing and addressing cyber-bullying

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

The college will actively discuss cyber-bullying with learners, explaining the reasons why it occurs, the forms it may take and what the consequences can be. [Class teachers/form teachers] will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Life Skills and Personal Development education, and other subjects where appropriate.

All staff, trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support learners, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the college will follow the processes set out in the college behaviour policy. Where illegal, inappropriate or harmful material has been spread among learners, 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 principal, and any member of staff authorised to do so by the principal (as set out in your behaviour policy – adapt to e.g. specify which staff are authorised), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or learners, 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 learners and staff. If the search is not urgent, they will seek advice from the principal.
- Explain to the learner why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the learner's co-operation.

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 staff member in conjunction senior leadership team 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 learner 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 and principal 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 learners 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 behaviour policy / searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on learners' 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, learners and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

KITE recognises that AI has many uses to help learners 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.

KITE will treat any use of AI to bully learners in line with our anti-bullying/behaviour policy.

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 by the college.

7. Acceptable use of the internet in college

All learners, parents/carers, staff, volunteers and trustees are expected to sign an agreement regarding the acceptable use of the colleges ICT systems and the intern. 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/professional purposes only, or for the purpose of fulfilling the duties of an individual's role.

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

8. Learners using mobile devices in college

- Lessons
- Tutorial group time

Any use of mobile devices in college by learners must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a learner may trigger disciplinary action in line with the college behaviour policy.

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).
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- 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 colleges terms of acceptable use, as set out in appendix 3.

If staff have any concerns over the security of their device, they must seek advice from DSL team or Principal.

10. How the college will respond to issues of misuse

Where a learner misuses the colleges ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT acceptable use. 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 colleges 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 disciplinary policy/staff behaviour code policy. 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 are at risk of online abuse.
- Learners 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 learners can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence learners to make the healthiest long-term choices and keep them safe from harm in the short term.

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

Trustees 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 child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on My Concern.

This policy will be reviewed every year by the principal. At every review, the policy will be shared with the trustee board. The review will be supported by a risk assessment that considers and reflects the risks learners 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 policy is linked to our:

- Child & Adult protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable use policy