BUSINESS & ENTERPRISE
The City of Leicester College

Online Safety and Acceptable Use Policy

Approved by:	Governors' T&L Committee	*Date:* 22/11/2021
Last reviewed on:	June 2020	
Next review due by:	November 2022	
Chair of Governors:	*J S Andrews*	

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school 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, anti-Semitism, 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 scam

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE) 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

[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. 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.

The policy also takes into account the National Curriculum computing programmes of study.

This policy should be read alongside the following TCOLC policies:

- Safeguarding and Child Protection Policy
- Behaviour for Learning Policy
- Anti-Bullying Policy
- PSHE Policy

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 Safeguarding Governor will attend regular meetings to discuss and receive regular updates from the Lead DSL and other appropriate staff about online safety.

The governor who oversees Safeguarding is John Andrews

All governors will:

Ensure that they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

Promote internet safety to parents/carers and provide updates on internet safety policies

3.2 The Headteacher

The Headteacher is Ken Vernon

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

The Head teacher delegates to the Lead DSL and ensures that they have the authority and time to carry out these duties effectively.

The Head teacher:

- Supports the following members of staff in their roles to create a culture of internet safety within the college:
  - Lead DSL
  - THE BOYD Project Leader
  - Information Manager
  - The ICT Manager

  This includes speaking to staff and students in support of the programme

- Ensures that the Governing Body is informed of issues and policies
- Ensures funding is available to support internet safety activities for both technical infrastructure and inset training
- Promotes internet safety across the curriculum

3.3 The Designated Safeguarding Lead (Lead DSL)

The Lead DSL is Jill Walton

The Lead DSL, supported by the Senior Deputy DSL and DSLs, takes the lead responsibility for online safety in school in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, BOYD Project Leader, Information Manager and Lead Education Technologist and other staff, as necessary, to address any online safety issues or incidents
- Working with the Head of ICT and PSHE and other leaders within the college responsible for the curriculum to establish and maintain a safe ICT learning environment.
- Develop and maintain knowledge of internet safety issues and disseminate this knowledge appropriately to all staff, students and relevant stakeholders.
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are appropriately recorded on CPOMs (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are recorded and dealt with appropriately in line with the school behaviour and child protection policies.
- Ensuring that any incidents of sexual violence and/or harassment, both online and offline are dealt with appropriately, in line with the school’s child protection policy, and maintaining an attitude of ‘it could happen here’

- Coordinating delivery of staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaise with other individuals and organisations, as appropriate, to ensure that those students being educated away from college premises will benefit from a safe ICT learning environment
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

Details of the school's DSL, Senior Deputy DSL and DSLs are set out in our child protection and safeguarding policy as well as relevant job descriptions.

3.4 The Bring Your Own Device Project Leader (BOYD)

BOYD Project Leader is Antony Tompkins.

The BOYD Project Leader is responsible for

- Coordinating delivery of staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Working with the Lead DSL, Information Manager and Lead Education Technologist and other staff, as necessary, to address any online safety issues or incidents
- Working with the Head of ICT and PSHE and other leaders within the college responsible for the curriculum to establish and maintain a safe ICT learning environment for students and staff
- Developing and maintaining knowledge of internet safety issues and disseminating this knowledge appropriately to all staff, students and relevant stakeholders
- Supporting the Lead DSL to develop and maintain additional policies and internet safety materials tailored to students and parents.

This list is not intended to be exhaustive.

3.5 Information Manager

The Information Manager is Lesley Bell.

The Information Manager is responsible for:

- Ensuring the school's ICT systems has appropriate levels of security in place, such as filtering and monitoring systems, and are reviewed on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Ensuring the schools ICT systems and networks are robust and resilient to cyber security attack.
- Ensuring that there is regular monitoring in place of the school's ICT systems. Any misuse is logged and reported as appropriate to DSL, Head Teacher or Head of Year.

- Ensuring Capita meet their contractual obligations with the school around ICT management.

3.6 ICT Manager

The ICT Manager is Charlotte Ryan.

The ICT Manager is responsible for:

- Working with the Information Manager and the school's ICT Management contractor (Capita) to put in place agreed security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Carry out regular security checks and monitoring of the school's ICT systems for indicators of misuse. To report any misuse as appropriate to DSL, Head Teacher or Head of Year.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.7 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 school's ICT systems and the internet (appendix 3), and ensuring that students follow the school's terms on acceptable use (appendices 1 and 2)

Working with the Lead DSL to ensure that any online safety incidents are reported to a member of the safeguarding team and recorded appropriately on CPOMS and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school 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.

3.8 Parents and Carers

Parents are expected to:

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

Parents 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 International

- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

3.9 Visitors and members of the community

Visitors and members of the community who use the school'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 3).

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum:

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

Relationships and sex education and health education in secondary schools

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **Key Stage 4** will be taught:

- 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

By the **end of secondary school**, 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 which 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 which 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 students with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. In particular:

- Parents and carers must be aware that as well as the computer internet access many games consoles offer internet connectivity and they need to be aware of the potential hazards relating to these items.
- Parent/carers must be aware of internet safety policies within college but also given practical strategies which could be adopted for the home.
- The college will ensure through information exchange that parent/carers are supported regarding internet safety as many are discouraged by their lack of knowledge with computers.
- Some parents/carers are unaware of the risks faced by the children when online and by education and support they will feel more able to guide and monitor their children's involvement with the Internet.

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

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

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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

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.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be during tutor time and assemblies.

Teaching staff are also encouraged to find opportunities to 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, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that 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 school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The Lead DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the Lead DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse includes an online element.

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

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

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

7. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school'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.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Students using mobile devices in school

Students are permitted to bring to school and use their iPad, issued to them through the TCOLC 1-to-1 iPad scheme. The use of these devices within school and at home is covered separately in the "TCOLC 1-to-1 iPad Acceptable Use Policy. Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Students are not permitted to use any other mobile device within school. They will be asked to acknowledge this and sign the mobile phone policy at the start of each academic year. If a student is seen with a device within school, they will be asked to put it away. If they should fail to comply with this, then the incident will referred to the behaviour team, who will confiscate the device. Parents will be informed and may be asked to collect the device.

9. Staff using work devices outside school

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 – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

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 LET

10. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and/or the child protection policy. 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 school'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 conduct, child protection policy and/or DfE Keeping Children Safe in Education (2021). The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which 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 (for example through emails, e-bulletins and staff meetings).

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
- Children can abuse their peers online through:
    - Abusive, 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 the risks up
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

All DSLs and the LET 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 child protection and safeguarding policy.

12. Monitoring arrangements

The Lead DSL logs behaviour and safeguarding issues related to online safety using CPOMS.

This policy will be reviewed every year by the Lead DSL. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy

Behaviour policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

Appendix 1: Student Acceptable Use of ICT Agreement

To ensure that all users of ICT facilities/equipment at The City of Leicester College are fully aware of their responsibilities when using information systems, they are asked to read this agreement and sign to say that they have done so when they join the college.

1. I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, Social networking and iPads.
2. I understand that all the software and hardware I will use for college purposes is the property of the City of Leicester College.
3. I understand that I must inform the ICT Technical Department of accounts to be closed and data to be maintained on departure from the College.
4. I understand that I must return all hardware and software in good working order on departure from the College.
5. I understand that it is a criminal offence to use College ICT systems for a purpose not permitted by its owner
6. I understand that the College may exercise its right to monitor the use of the College's information systems
7. I understand that the College may exercise its right to monitor the use of the College's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorized use of the College's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorized or unlawful text. imagery or sound.
8. I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
9. I will ensure that electronic communications with pupils including email, Instant Messaging and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
10. I will use the ICT facilities responsibly and not waste College resources.
11. I will ensure chat students do not use College ICT equipment to play games for leisure purposes or send chain, junk or abusive or bulk emails.
12. I will ensure that students use ICT equipment appropriately and that students leave the computers, labs and other devices in a clean, usable state.
13. I will ensure that students do not disconnect machines or attempt to change the mice or keyboards and will not attempt to repair faults but will report all faults to the ICT Technical Department.
14. I will report any faulty equipment to the ICT Technical Department using the agreed procedure.

Data Protection

1. I understand that sharing passwords may lead to breaches of security and **I agree not to share any passwords or restricted usernames with anyone other than an authorized person.**
2. I will not destroy another user's files, create or introduce a virus to the College network.
3. I understand that I have a legal responsibility to maintain the security of work related data and will ensure that personal data is stored securely **(encrypted and by using a password at all times)** and is used appropriately, whether in College, taken off the College premises or accessed remotely.
4. I understand that the College uses software to monitor inappropriate or illegal use of ICT technologies which may result in screen shots from network computers being captured if they contain trigger words or phrases.
5. I recognize that information and software available via the network is subject to copyright and or restrictions on its use.
6. I will respect copyright and intellectual property rights.
7. I acknowledge that all Data scored on the College network is the property of the College.

Signed: Date:

Name: Form:

Appendix 2: Staff Acceptable Use of ICT Agreement

To ensure that all adult users of ICT facilities/equipment at The City of Leicester College are fully aware of their responsibilities when using information systems, they are asked to read this agreement and sign to say that they have done so at the start of each year.

Professional Responsibility

1. I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, Social networking and iPads.
2. I understand that all the software and hardware I will use for college purposes is the property of the City of Leicester College.
3. I understand that I must inform the ICT Technical Department of accounts to be closed and data to be maintained on departure from the College.
4. I understand that I must return all hardware and software in good working order on departure from the College.
5. I understand that it is a criminal offence to use College ICT systems for a purpose not permitted by its owner
6. I understand that the College may exercise its right to monitor the use of the College's information systems
7. I understand that the College may exercise its right to monitor the use of the College's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorized use of the College's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorized or unlawful text. imagery or sound.
8. I will not install any software or hardware without permission and will ensure license requirements are complied with fully.
9. I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
10. I will ensure that electronic communications with pupils including email, Instant Messaging and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
11. I will use the ICT facilities responsibly and not waste College resources.
12. I will ensure chat students do not use College ICT equipment to play games for leisure purposes or send chain, junk or abusive or bulk emails.
13. I will ensure that students use ICT equipment appropriately and that students leave the computers, labs and other devices in a clean, usable state.
14. I will ensure that students do not disconnect machines or attempt to change the mice or keyboards and will not attempt to repair faults but will report all faults to the ICT Technical Department.
15. I will report any faulty equipment to the ICT Technical Department using the agreed procedure.

Data Protection

1. I understand that sharing passwords may lead to breaches of security and **I agree not to share any passwords or restricted usernames with anyone other than an authorized person.**
2. I will not destroy another user's files, create or introduce a virus to the College network.
3. I understand that I have a legal responsibility to maintain the security of work related data and will ensure that personal data is stored securely **(encrypted and by using a password at all times)** and is used appropriately, whether in College, taken off the College premises or accessed remotely.
4. I understand that the College uses software to monitor inappropriate or illegal use of ICT technologies which may result in screen shots from network computers being captured if they contain trigger words or phrases.
5. I recognize that information and software available via the network is subject to copyright and or restrictions on its use.
6. I will respect copyright and intellectual property rights.
7. I acknowledge that all Data scored on the College network is the property of the College

Signed: Date:

Name: Role:

Appendix 3: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways students can abuse their peers online?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	