Online Safety and Acceptable Use Policy

2024 - 2025

Approved by:	Governing Board	Date: 27.01.2025
Last reviewed on:	January 2024	
Next review due by:	November 2025	
Chair of Governors:	*JS Andrews*	

1. Aims

At The City of Leicester College, we acknowledge and celebrate that we live in an exciting digital world full of possibility and wonder. The use of technology and the internet enriches our ambitious academic and co-curriculum, inspiring our students to broaden their thinking and to deepen their knowledge of the world we live in. However, we recognise that without effective and appropriate education, training, systems, support, and processes in place our students, staff and stakeholders may be vulnerable to the dangers and risks that the internet can pose.

This policy aims to:
- Set guidelines and rules on the use of school ICT resources for staff, students, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching students safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, students, volunteers, contractors and visitors. Breaches of this policy may be dealt with under our staff code of conduct.

2. Legislation and Guidance

- This policy refers to, and complies with, the following legislation and guidance:
- Keeping Children Safe in Education (2024)
- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges
- The Prevent duty: safeguarding learners vulnerable to radicalisation

3. Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service
- **Users:** anyone authorised by the school to use the school's ICT facilities, including governors, staff, students, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

4. Roles and Responsibilities

4.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the Lead DSL, Jill Walton, to account for its implementation. The governor who oversees Safeguarding, including online safety, is Naresh Chauhan.

All governors will:
- Ensure 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 2).
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students 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 children in all situations, and a more personalised or contextualised approach may often be more suitable.

In addition to the above, the Governor who oversees safeguarding 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.
- Make sure all staff receive regular online safety updates as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- 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).
- Ensure children are taught how to keep themselves and others safe, including keeping safe online.
- Ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The governor who oversees Safeguarding will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those 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.

This list is not intended to be exhaustive.

4.2 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 Headteacher:
Supports the following members of staff in their roles to create a culture of internet safety within the college:
- Lead DSL
- Strategic Information Lead
- 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.

This list is not intended to be exhaustive.

4.3 The Designated Safeguarding Lead (Lead DSL)
The Lead DSL is Jill Walton.
The Lead DSL, supported by the Senior Deputy DSLs and DSLs, takes the lead responsibility for online safety in school. Details of the school's DSL, Senior Deputy DSLs and DSLs are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL is responsible for:
- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher 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 school devices and school networks.
- Working with the ICT manager to make sure the appropriate systems and processes are in place.
- Working with the Headteacher, Strategic Information Lead, ICT Manager, and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school's child protection policy.

- Ensuring that any online safety incidents are appropriately recorded on CPOMs 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.
- Working with the curriculum leaders to establish and maintain a safe online learning environment, including the regular review of frequently used websites and the sharing of this information with parents.
- Develop and maintain knowledge of internet safety issues and disseminate this knowledge appropriately to all staff, students, and relevant stakeholders.
- Coordinating delivery of staff training on online safety.
- 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.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- 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.

4.4 Strategic Information Lead
The Strategic Information Lead is Lesley Bell, responsible for:
- Ensuring the schools ICT systems meet the digital and technology standards as set out by the Department for Education.
- 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. To undergo internal audits as required by the Aspire Trust. To achieve and maintain Cyber Essentials accreditation through annual audits. Cyber Essentials is a government-backed, industry-supported scheme to help organisations protect themselves against common online threats.
- 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 meets their contractual obligations with the school around ICT management.
- Ensuring the school's network, data and systems have appropriate levels of backup in place.
- Provide regular training and raise general awareness on working safely online, being cybersecure and general data protection matters.

This list is not intended to be exhaustive.

4.5 ICT Manager
The ICT Manager is Charlotte Ryan, responsible for:
- Working with the Strategic Information Lead 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.
- Ensure appropriate filtering is in place to block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Oversee IT technicians to ensure all ICT devices are running up-to-date software.
- Support Strategic ICT Lead and Capita with the annual Cybersecurity audit.
- Manage access rights across the network (e.g. SharePoint, O drive) to ensure staff and students are appropriately accessing only what they need to.
- Ensuring that any online safety incidents are appropriately recorded on CPOMs and dealt with appropriately in line with this policy.

This list is not intended to be exhaustive.

4.6 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 2), and ensuring that students follow the school's terms on acceptable use (appendices 1 and 2).

- Knowing that the DSL 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 recording appropriately on CPOMS and notifying the ICT Manager, Charlotte Ryan.
- Following the correct procedures as set out by the ICT Manager if they need to bypass the filtering and monitoring systems for educational purposes.
- 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'.
- Utilising Netsupport to monitor use of devices within the classroom.

All staff are expected to read and agree to college's Acceptable Use Agreement

This list is not intended to be exhaustive.

4.7 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

Parents are expected to read and agree to college's Acceptable Use Agreement.

This list is not intended to be exhaustive.

4.8 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 2).

4.9 Students
Students are expected to:
- Students should not attempt to install or store programs of any type on the computers.
- Respect ICT equipment owned by The City of Leicester College and should not cause intentional damage, e.g., Damaging, disabling, or otherwise harming the operation of computers, or intentionally waste resources.
- Only use the computers for educational purposes.
- Mobile equipment (e.g., laptops, tablets) should not be connected to the school network without the permission of the ICT department.
- Keep their passwords protected and should never share passwords or use someone else's logon name or password.
- Always get permission before revealing your home address, telephone number, school name, or picture to people you meet on the internet.
  To uphold our Character expectations both within the college and the local community. This means, we are moral characters who serve our community and act with respect and civility and do not use technology to cause harm by bullying, harassing, discriminating, offending insulting and/or abusing.
- Ensure access to the internet is for study and/or for college authorised/allowable activities.
- Only access suitable material – using the internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene, or abusive is not permitted.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- Report content, e.g., emails containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of staff. The sending or receiving of an email containing content likely to be unsuitable for children or schools is strictly forbidden.

Students are expected to read and agree to college's Acceptable Use Agreement.

This list is not intended to be exhaustive.

5. Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 5.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its students, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):
  - During assessments, including internal and external assessments, and coursework
  - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

This is not an exhaustive list. The school reserves the right to amend this list at any time. The [headteacher or any other relevant member of staff] will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

5.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

5.2 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 Safeguarding and Child Protection. 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, Safeguarding and Child Protection Policy, including the school's low-level concern policy and/or DfE Keeping Children Safe in Education (2024). 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.

6. Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel, e.g. ICT Manager, Lead DSL may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The City of Leicester College we publish comprehensive information about which monitoring and filtering software is used to keep both students and staff safe on its website. We also share detailed guidance with parents regarding how it ensures we meet the DFE standard and how we audit online use across use across the curriculum.

The school monitors ICT use in order to:
- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our governing board is responsible for making sure that:
- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

7. Staff access to ICT facilities

The school's ICT manager manages access to the school's ICT facilities and materials for school staff (including governors, contractors, volunteers and trainees) That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT manager.

7.1 Use of phones and email

- The school provides each member of staff with an email address.
- This email account should be used for work purposes only.
- All work-related business should be conducted using the email address the school has provided.
- Staff must not share their personal email addresses with parents/carers and students, and must not send any work-related materials using their personal email account.
- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
- If staff receive an email in error, the sender should be informed and the email deleted. If the email contains

sensitive or confidential information, the user must not make use of that information or disclose that information.
- If staff send an email in error that contains the personal information of another person, they must inform the [network manager immediately and follow our data breach procedure.
- Staff must not give their personal phone number(s) to parents/carers or students.
- Staff must use phones provided by the school to conduct all work-related business.
- School phones must not be used for personal matters.
- Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 5.

7 .2 Personal Use
Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Headteacher may withdraw or restrict this permission at any time and at their discretion.
Personal use is permitted provided that such use:
- Does not take place during contracted hours
- Does not constitute 'unacceptable use', as defined in section 5
- Takes place when no students are present
- Does not interfere with their jobs, or prevent other staff or students from using the facilities for work or educational purposes
Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).
Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 6). Where breaches of this policy are found, disciplinary action may be taken.
Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's mobile phone policy

7 .3 Personal social media accounts
Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

7 .4 Staff device security
At The City of Leicester 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 – always installing 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 2.

If staff have any concerns over the security of their device, they must seek advice from the ICT Manager.
7.5 Staff Training
All new staff members of staff, including governors, 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 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 ICT Manager 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. All staff undergo annual cyber security and data protection training.

All Governors new to role will receive online safety training as part of their induction and thereafter Governors will receive regular safeguarding training, including safer internet use to ensure they remain up to date about the risks that students face and indeed themselves. Volunteers will receive appropriate training and updates, if applicable.

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

8. Student access to ICT facilities

The school's ICT manager manages access to the school's ICT facilities and materials for students That includes, but is not limited to:
- Computers, tablets and other devices
- Access permissions for certain programmes or files

Students will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Students who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT manager.

- Computers and equipment across the college are available to students only under the supervision of staff
- Specialist ICT equipment, such as that used for design and technology, must only be used under the supervision of staff
- Sixth-form students can use the computers independently, for educational purposes only. P16

8.1 Students using personal devices in school

At the City of Leicester College, 6th Form students are permitted to bring to school and to use their devices in designated areas e.g. the Library. Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school's Behaviour Policy and may result in the confiscation of their device.

Y7-11 students are not permitted to use mobile devices within school, unless specifically directed by a teacher for learning purposes. We acknowledge that many parents/carers feel reassured by their child having a mobile phone for the commute to and from school, therefore for students in Years 7-11 we expect students to have their mobile phones and associated technology, e.g. air pods, out of sight and switched off, as soon as students have entered the school building in the morning. If a student is seen with a mobile device within school and permission has not been granted, then the phone will immediately be confiscated until the end of the school day and a correction issued. If the student fails to comply with this, they will be issued a sanction in line with our college behaviour policy and appropriate to the level of chosen refusal and disruption to the college community.

8.2 Examining electronic devices

Members of staff as identified in the school's behaviour policy 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 school 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 / Lead DSL / Pastoral Senior Leaders].
- 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 cooperation.

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 school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to Headteacher and/or Lead DSL and/or Pastoral Senior Leader 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 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 (or equivalent) 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
- The college's Behaviour for Learning policy, which includes guidance on searches and confiscation.

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

9. Educating students about online safety

The City of Leicester College will teach students about online safety through the academic and co-curriculum. Students across years 7-11 will be taught about online safety as part of their TCOLC Character programme and will receive more formalised lessons through the ICT and PSHE curriculums.

9.1 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, radicalization, 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

9.2 The PSHE Curriculum

The PSHE curriculum will be the main vehicle to teach our students about the risks and dangers they may face online. At The City of Leicester College, the PSHE curriculum takes its guidance from what all schools have to teach in terms of online safety and associated themes and topics from, the guidance on relationships education, relationships and sex education (RSE) and health education.

Students in Years 7-9 (KS3), 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.

10. Educating parents about online safety

The City of Leicester College acknowledge that many parents/carers are concerned about internet safety but feel discouraged often because of their own knowledge with computers and mobile technology. 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.
We will aim to raise parents' awareness of internet safety through information exchange such as signposting and letters home other information via our website. This policy will also be shared with parents.

Online safety information will also be available in our reception and a member of the safeguarding team will always be available for parents/carers to discuss internet with on Parents' Evenings.
The school will let parents know:
- What systems the school 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 school (if anyone) their child will be interacting with online.
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.

11. Data Security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and students. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.
Staff, students, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:
- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

11.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure, We require that all passwords are a minimum of 8 characters and include a capital letter, numbers and have not been used for the past 23 occasions.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or students who disclose account or password information may face disciplinary action.

All staff will use the password manager required by the ICT manager to help them store their passwords securely.

Teachers will generate passwords for students using the required password manager or generator and keep these in a secure location in case students lose or forget their passwords.

11.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices used by staff or Post 16 using the school's network must all be configured in this way.

11.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

11.4 Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as student information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT manager.

12. Cyber-bullying

12 .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 City of Leicester's Behaviour for Learning Policy.)

12.2 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 City of Leicester College, 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 our TCOLC Character tutor time sessions and PSHE lessons.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum and/or TCOLC Character Pillars to cover cyber-bullying. The school also ensures parents/carers understand the signs cyber-bullying and know, 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 and/or will also follow procedures as set out in the Safeguarding and Child Protection 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.

13. Artificial Intelligence

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 City of Leicester 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. The City of Leicester College will treat any use of AI to bully students in line with our 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 school/trust. Appropriate guidance on using AI tools will be given as they are introduced. Under no

circumstances should personal data be entered into an AI Tool. Where found to be done, this would be treated a data breach as per the Data Protection Policy.

14. Links with other policies

The City of Leicester College recognises that online safety is a matter for the whole school and its community. Therefore, our Online Safety and Acceptable Use Policy should not be read in isolation and should be viewed in conjunction with the following college policies:

- Safeguarding and Child Protection Policy
- Behavior Policy
- Anti-bullying policy
- Staff Code of Conduct
- Parent and Carers Code of Conduct
- Low-level concern Policy
- Complaints Procedure
- PSHE Policy
- Anti-bullying Policy
- GDPR Policy
- Exam Policy
- Personal Electronic Device Policy

This policy will be reviewed every year by the Lead DSL, Strategic Information Manager, and ICT Manager. At every review, the policy will be shared with the Governing Board for approval.

Appendix 1: Student Acceptable Use of ICT Agreement

THE CITY OF LEICESTER COLLEGE

To ensure that all student 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.

Name of Student:

I will read the following expectations and rules in the acceptable use agreement policy, if I do not understand any of these expectations and/or rules I will ask a member of staff at the college to explain them to me before I sign this agreement.

As a student member of the City of Leicester College:
- I appreciate that ICT includes a wide range of systems, including iPads, mobile phones, PDAs, digital cameras, email, social networking, and that ICT use may also include personal ICT devices when used for college business.
- 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.
- I understand that sharing passwords may lead to breaches of security and I agree not to share any password or restricted usernames with anyone other than an authorised person, e.g., a college ICT technician.
- I will 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.
- I will not create, link to, or post any material that is pornographic, offensive, obscene, or otherwise inappropriate, especially about any other member of the TCOLC community. I understand that if I do so that I will face serious sanction.
- I will tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others.
- I will not use any inappropriate language when communicating online, including in emails.
- I will not log in to the school's network using someone else's details.
- I will not destroy another user's files, create, or introduce a virus to the College network.
- I will not attempt to 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.
- I recognise that information and software available via the network is subject to copyright and/or restrictions on its use.
- I will respect copyright and intellectual property rights.
- I acknowledge that all Data stored on the College network is the property of the College.
- I understand that I must inform the ICT Technical Department of accounts to be closed or data to be maintained and hardware to be handed in on departure from the College.
- I will ensure that I leave the computers in a clean, usable state and report any faulty equipment to the ICT Technical Department.
- I will ensure that I do not eat or drink in computing rooms, labs, or areas where ICT equipment is present.
- I understand that it is a criminal offence to use College ICT systems for a purpose not permitted by its owner.
- I will not open any attachments in emails, or follow any links in emails, without first checking with a teacher.
- I will not arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

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 unauthorised use of the College's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery, or sound.

Signed: **Date:**

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 and accessing the internet in the college, or outside the college on a work device they are asked to read this agreement and sign to say that they have done so at the start of each year.

Name of staff member/governor/volunteer/visitor:

I will read and adhere to the following expectations and rules in the acceptable use agreement policy

- I appreciate that ICT includes a wide range of systems, including iPads, mobile phones, PDAs, digital cameras, email, social networking, and that ICT use may also include personal ICT devices when used for college business.
- 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.
- I understand that sharing passwords may lead to breaches of security and I agree not to share any password or restricted usernames with anyone other than an authorised person.
- I will not destroy another user's files, create, or introduce a virus to the College network.
- I recognise that information and software available via the network is subject to copyright and/or restrictions on its use.
- I will not install any software or hardware without permission and will ensure license requirements are complied with fully.
- I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me, they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- 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 (using a password at all times) and is used appropriately, whether in college, taken off the College premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will ensure that electronic communications with students including email, Instant Messaging and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- 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.
- I acknowledge that all Data stored on the College network is the property of the College.
- I understand that I must inform the ICT Technical Department of accounts to be closed or data to be maintained and hardware to be handed in on departure from the College.
- I will use the ICT facilities responsibly and not waste College resources.
- I will ensure that students do not use College ICT equipment to play games for leisure purposes or send chain, junk or abusive or bulk emails.
- I will ensure that students leave the computers in a clean, usable state and report any faulty equipment to the ICT Technical Department.
- I will ensure that students do not eat or drink in computing rooms, labs, or areas where ICT equipment is present.
- 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.
- I understand that it is a criminal offence to use College ICT systems for a purpose not permitted by its owner.
- I will always use the school's ICT systems and internet responsibly and ensure that students in my care do so too.

Signed (staff member/governor/volunteer/visitor):	Date: