

# Online Safety Policy

|                                |                                                      |
|--------------------------------|------------------------------------------------------|
| <b>Policy Family:</b>          | Corporate Governance and Legal Frameworks            |
| <b>Reference Code:</b>         | GOV12                                                |
| <b>Issue Number:</b>           | 5                                                    |
| <b>Originator:</b>             | Assistant Principal Student Experience and Wellbeing |
| <b>Responsible Manager:</b>    | Assistant Principal Student Experience and Wellbeing |
| <b>Committee for Approval:</b> | Safeguarding/Corporation Board                       |
| <b>Approval Date:</b>          | May 2026                                             |
| <b>Issue Date:</b>             | May 2026                                             |
| <b>Review Due:</b>             | May 2027                                             |

**Impact Assessment Status:** In preparing the Policy, any potential disproportionate impact it might have upon individuals with protected characteristics, as defined in the Equality Act 2010, have been carefully considered. It is the conclusion of the College Group that the Policy does not adversely impact on individuals with any of the protected characteristics.

## Contents

|                                                                |    |
|----------------------------------------------------------------|----|
| Aim .....                                                      | 3  |
| Scope .....                                                    | 3  |
| Policy Statements .....                                        | 4  |
| Implementation.....                                            | 11 |
| Monitoring.....                                                | 13 |
| Associated Information and Guidance .....                      | 13 |
| Related Chesterfield College Group Policies and Documents..... | 14 |

## Aim

The Online Safety Policy aims to ensure that:

1. Members of the Chesterfield College Group community are safeguarded and protected whilst engaged in online activity.
2. There is a commitment across the College Group to identify and embed approaches to educate and raise awareness of online safety.
3. Staff work safely and responsibly to role model positive behaviour online and to manage professional standards and practice when using technology.
4. The College Group is effective in responding to online safety concerns.

The College Group identifies that the issues classified within online safety are considerable but can be broadly categorised into four areas:

1. **Content:** being exposed to illegal, inappropriate, inaccurate, misleading or harmful material.
2. **Contact:** being subjected to inappropriate and/or harmful online interaction with others.
3. **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
4. **Commerce:** being exposed to inappropriate commercial advertising, online gambling services or scams.

## Scope

This policy and associated operating procedures apply to Chesterfield College, which includes our subsidiary companies: Training Services 2000 Ltd, Learning Unlimited ATA Ltd, Recruit Unlimited Ltd and Chesterfield College Enterprises Ltd.

The policy applies to all members of the College community including staff, students, apprentices, parents and carers, and other college users, including volunteers, external contractors, visitors, remote students, and employers where students or apprentices have work placements or are engaged in work-based learning.

The policy is part of the Safeguarding Policy Family, providing specific guidance around the risks associated with online activity and a framework with which to protect all college users from potential harm online.

The policy applies to all access to the internet and use of technology, including personal devices, or where students, apprentices, staff, or other individuals have been provided with College Group issued devices for use off-site, such as laptops, tablets, or mobile phones. The college recognises that in some cases online risk will be minimised by enforcing expectations around behaviour and codes of conduct, alongside teaching and learning in relation to online

safety, and that not all risks can be flagged to the Safeguarding Team through web-filtering unless the individual is accessing the internet via the college network. Where this is the case however, daily web filtering reports mapped against a broad set of search terms reflecting potential risk or inappropriate content, are received and monitored by the safeguarding team. Where a potential risk or inappropriate content is received, appropriate discussions will take place with individuals by the safeguarding team (students/apprentices) or the Assistant Principal People and Culture (staff).

## Policy Statements

The Chesterfield College Group recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all students and apprentices are protected from potential harm online, whilst also recognising that the internet and associated devices, such as computers, laptops, tablets, mobile phones, and games consoles, are an important part of everyday life. The college believes that students and apprentices should be empowered to build resilience and to develop strategies to manage and respond well to online risk.

This policy has been developed in line with the College's commitment to foster equality, diversity and inclusion in accordance with the Equality Act 2010.

Students and apprentices will be supported to:

- Engage in age, curriculum, and level appropriate online safety education opportunities through the Empower Personal Development Curriculum.
- Read and adhere to the IT Acceptable Use Policy and the Student Code of Conduct.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves safe online.
- Seek help from a trusted adult if there is an online safety concern.

Staff will be supported to:

- Access appropriate training opportunities related to online safety.
- Understand online safety risk and how to report any concerns through usual safeguarding reporting arrangements.
- Be familiar with and adhere to other college policies such as the IT Acceptable Use Policy and the Staff Code of Conduct.
- Conduct themselves with professionalism and integrity whilst using online platforms in line with the requirements outlined in this policy.

The Chesterfield College Group Senior Management Team, in conjunction with ICT Services and the Designated Safeguarding Lead, have ensured that the College Group has age and ability appropriate filtering and monitoring in place to limit exposure to online risk whilst on college premises.

The College are aware of the need to prevent 'over-blocking' as this may unreasonably restrict what can be taught with regards to online activities and safeguarding.

## **Managing Internet Access**

Staff, students, apprentices, and visitors will be signposted to the IT Acceptable Use Policy (INF02) on first use of college internet systems, and the policy's Simplified Code will be regularly promoted across the college community.

## **Filtering**

The college uses an appropriate filtering system which blocks sites that are deemed to be harmful, distracting, or unnecessary for the fulfilment of a complete learning experience. The college blocks all sites on the Internet Watch Foundation (IWF) list. Some sites will be 'soft-blocked', allowing access whilst being accompanied by a warning, whilst other sites will be inaccessible through a 'hard-block'.

Staff, students, and apprentices are encouraged to report unsuitable sites that are discovered to be accessible to ICT Services.

Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the Police, or the Child Exploitation and Online Protection Command (CEOP).

## **Monitoring**

Internet usage is appropriately monitored on all College Group provided internet enabled devices, in line with data protection, human rights, and privacy legislation. Any identified concern is reviewed by the Safeguarding Team in line with the college's Safeguarding Policy and Procedures (GOV05).

Where a risk assessment indicates the need, a higher level of monitoring or restriction may be implemented in order to keep students safe.

## **Use of Personal Devices and Mobile Phones**

Chesterfield College Group recognises that personal communication through mobile technologies is an accepted part of everyday life for students, apprentices, staff, and other members of the wider college community, but that technologies need to be used safely and appropriately within the college setting.

Members of the College community should adhere to the IT Acceptable Use Policy (INF02) and staff/student codes of conduct in their use of personal devices and mobile phones on college premises (and, to a reasonable extent, outside of College premises). Students/apprentices should also follow any locally issued instructions within the classroom or workplace setting (apprentices).

## **Social Media**

Chesterfield College Group will control staff and student access to social media whilst using College Group provided devices and systems on site.

The College Group expects all members of staff to use social media safely and responsibly. Concerns regarding staff conduct on social media platforms should be raised with the People

and Culture Team. Where the concern is of a safeguarding nature a report should be made following the processes for allegations against staff as detailed in the college's Safeguarding Policy and Procedures (GOV05).

As part of active social media engagement, the College will monitor the internet for public postings about the College.

Where parents or carers express concerns about the College on social media they will be encouraged to make direct contact with the College to try and resolve the matter privately. They will also be informed of the College's complaints procedures where necessary.

Safe and appropriate use of social media will form part of the educational approach to students and apprentices across the College Group. Students and apprentices will be advised:

- To consider the benefits and risks of sharing personal details on social media platforms that could identify them and their location.
- To only approve and invite known friends on social media platforms and to deny access to others by making profiles private.
- That they should not meet online friends without considering their personal safety and, where under 18, informing a trusted adult.
- To use secure passwords on all social media platforms.
- To only use social media platforms that are appropriate for their age and ability.
- How to block unwanted communications.
- How to report concerns to both the college and to external agencies.

Any concerns regarding student or apprentice conduct on social media should be approached by following guidance in the appropriate policy:

- Student Code of Conduct.
- Student and Apprentice Disciplinary Policy (TLA03).
- Anti-Bullying Policy (GOV07).
- Safeguarding Policy (GOV05).

Organisational use of social media should be guided by the Brand and Communications Team. This includes setting up social media groups using the college name and those intended to promote the college offer. All staff should seek advice and guidance from the Brand and Communications Team prior to the instigation of any organisational social media use.

### **Safer Use of Technology in the Learning Environment**

Chesterfield College Group uses a wide range of technology in the delivery of its services. This includes, but is not limited to:

- Computers, laptops, tablets, and other digital devices.
- Learning platforms, including the Virtual Learning Environment (VLE) and OneFile.
- Email and other communication systems.
- Games consoles and other games-based technologies.
- Digital cameras, web cameras, video conferencing systems, and video cameras.

All devices provided by the College Group must be used in accordance with the IT Acceptable Use Policy and with appropriate safety and security measures in place. All internet connected devices, including College Group issued mobile phones, will be managed using mobile and other device management software.

Staff must always evaluate websites, online resources, tools, and apps fully before use in the learning environment or recommendation for home use.

Chesterfield College Group will take necessary steps to ensure that search tools provided are appropriate, for example by enforcing safe search when using Google. Staff should not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral. Even web content which is legal may be considered of sufficiently bad taste to fall within this prohibition. As a general rule, if any person (whether they intended to view the page or not) might be offended by the contents of a page, or the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

### **Teaching and Learning of Online Safety**

The college will establish and embed effective learning around online safety through the Empower Personal Development Curriculum by:

- Ensuring initial education regarding safe and responsible internet use occurs during induction and within the first six weeks of each new academic year.
- Ensuring ongoing online safety education is embedded within the Empower Personal Development Curriculum delivered by curriculum teams.
- Reinforcing online safety messages whenever technology or the internet is used.
- Educating students and apprentices of all ages and levels in the effective use of the internet to research, including the skills of knowledge location, retrieval, and evaluation.
- Educating students and apprentices to be critically aware of the materials they read online and supporting students and apprentices to learn how to validate information before accepting its accuracy.

The education described above will be flexible and differentiated between learning programmes where altered, more specific, or less intensive delivery is required. Specialist technical support will be provided to groups where access to the internet and/or technology would ordinarily be restricted but is essential for learning.

Students and apprentices will be supported to understand the acceptable use of IT facilities in a way that suits their age and ability by:

- Displaying the Acceptable Use Policy Simplified Code in all locations where students and apprentices may access the internet using college-provided technology.
- Informing students and apprentices that network and internet usage will be monitored for safety and security in accordance with relevant legislation.
- Where practicable, peer education approaches will be implemented.

- Using support, such as external visitors, to complement the college's internal online safety education approach.

**If students and apprentices feel as though they require any further support, they should approach a Tutor or the IT department.**

### **Vulnerable Students**

The college recognises that some students and apprentices are more vulnerable online due to a range of factors including, but not limited to:

- Care Experienced young people.
- Special educational needs and disabilities (SEND).
- Mental health support needs.
- English as an additional language.
- Experience of trauma or loss.

When developing and implementing online safety education, specialist support will be sought from staff, including those responsible for safeguarding, supporting mental health, and SEND.

### **Awareness and Engagement with Parents and Carers of Students and Apprentices under 18 or those with an Education, Health and Care Plan (EHCP)**

The college recognises that parents and carers have an essential role to play in enabling young people to become safe and responsible users of the internet and associated technologies.

The college will, where appropriate:

- Provide information relating to pertinent issues around online safety to the parents and carers of students and apprentices under the age of 18 and those with an EHCP.
- Publish this policy on the college website and publicise online safety messages on social media platforms and through the Parents Hub.

**If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Safeguarding Team via [ccsafe@chesterfield.ac.uk](mailto:ccsafe@chesterfield.ac.uk) or 01246 500688**

### **Training and Engagement with Staff**

As part of wider induction activity new staff are made aware of the Safeguarding Policy Family, including the Online Safety Policy.

New and existing staff will be made aware of the following:

- IT systems are monitored, and activity can be traced back to individual users. Staff will be reminded to behave professionally and in accordance with College Group policies when accessing college systems and devices.



- Online conduct outside of the college, including personal use of social media, could have an impact on their professional role and the reputation of both themselves and the College.
- Appropriate safeguarding reporting in relation to online safety concerns.

## **Managing Email**

The college's email system will be managed in line with data protection legislation and other internal policies, such as the IT Acceptable Use Policy (INF02), Information Security Policy (INF01), and Codes of Conduct. Consideration should be given to the following:

- The forwarding of chain messages is not permitted.
- Spam or junk mail should be placed in the appropriate 'Junk Email' folder for processing by ICT Services.
- Any personal or sensitive information should be sent externally using the college-approved ZendTo secure file transfer service, and the sending of personal and sensitive information via email should be avoided.
- College Group generated email addresses should not be used to set up personal social media accounts.

The receipt of any offensive communication should be reported immediately to the recipient's Personal Tutor (if received by a student or apprentice) or Line Manager (if received by a member of staff). When safeguarding is a factor, the Safeguarding Team should be notified immediately.

Staff are encouraged to have an appropriate work/life balance when checking and responding to email, especially when communicating with students, apprentices, parents and carers outside of normal working hours. Whereby an email is received outside of usual working hours, there is no expectation on staff, students, apprentices, parents and carers to respond outside of the usual working hours of the college.

## **Management of Learning Platforms and Applications Used to Track Student and Apprentice Progress**

The college uses several learning platforms and other software packages to enable the tracking of student and apprentice progression.

The college may, as part of its normal business practices, choose to adopt new platforms, replace existing platforms with an appropriate substitute, or cease using a platform altogether.

The use and content of learning platforms will be monitored, including any messaging, communication, and publishing facilities.

Only current students, apprentices, and staff will have access to learning platforms. Accounts are disabled once a student, apprentice, or member of staff leaves the College Group.

All tracking systems holding student or apprentice data, images, videos, or other digital information are risk assessed prior to use and on an ongoing basis, to ensure that all

information is stored securely and in accordance with data protection legislation. To safeguard student and apprentice data:

- Staff will only use college issued devices to access systems that record and store student and apprentice personal details, attainment, and other digital data.
- Devices that are taken off-site will be appropriately encrypted to mitigate the risk of a data security breach in the event of loss or theft.
- All users will be advised regarding appropriate safety measures, such as the use of strong passwords and logging out of systems when they are not in use.

### **Reducing Online Risks**

The college recognises that the internet is a constantly changing environment with new apps, devices, websites, and material emerging at a rapid pace.

The college will:

- Regularly review the methods used to identify, assess, and minimise online risk.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessment before any new technology is used within the College Group.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Recognise that due to the global and ever-changing nature of the internet it will not always be possible to ensure that unsuitable material cannot be accessed via the college's systems and networks.

All members of the college community are aware of the college's expectations regarding safe and appropriate online behaviour both whilst at college and in their personal lives, and the importance of not posting or searching online any content, comments, images, or videos which could cause harm, distress, or offence.

### **Responding to Online Concerns**

All responses to concerns raised will be managed within the provisions set out within the college's Safeguarding Policy (GOV05) and Anti-Bullying Policy (GOV07). Concerns may include (this list is not exhaustive):

- Student or apprentice wellbeing.
- Online sexual violence and/or sexual harassment between children.
- Sharing nudes and semi-nudes.
- Online child sexual abuse and exploitation.
- Child Sexual Abuse Material (CSAM).
- Cyberbullying.
- Online hate.

## Implementation

The Designated Safeguarding Lead has lead responsibility for safeguarding and child protection, including in relation to online safety. However, all members of the college community have an important role to play with regards to online safety.

The Safeguarding and Wellbeing Manager (Deputy Designated Safeguarding Lead), supported by the Designated Safeguarding Lead will:

- Act as a key point of contact for all online safety issues in line with broader safeguarding arrangements.
- Work alongside curriculum staff to ensure that online safety is recognised as part of the college's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure that all staff access regular, up-to-date, and appropriate safeguarding training which includes online risks for all cohorts, including those with existing vulnerabilities such as special educational needs and disabilities (SEND).
- Keep up to date with current research, legislation, and trends regarding online safety and communicate this as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to staff, students, apprentices, parents, carers, and the wider community through a variety of channels and approaches.
- Maintain records of online safety concerns, including actions taken, as part of the college's safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends and use the data to update the college's educational response, policies, and procedures.
- Report online safety concerns to the Senior Management Team and Safeguarding Committee via standardised reporting.
- Meet with the safeguarding lead governor through an organised schedule of visits/interactions.
- Participate in the reviewing of the College's online safety policies.

The Designated Safeguarding Lead and the Safeguarding Team should be trained in online safety issues and be aware of the potential for safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate online contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber crime.
- Online bullying.

The Senior Leadership Team and Governing Body will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local requirements and recommendations.
- Ensure that there are appropriate and up-to-date policies in place regarding online safety, including a staff code of conduct, student code of conduct, and IT acceptable use policy.
- Ensure that online safety is embedded in curriculum delivery to enable all students and apprentices to develop an age and level appropriate understanding of online safety.
- Support the Safeguarding Team by ensuring that they have sufficient time and resources to fulfil their safeguarding responsibilities.
- Ensure that there are robust reporting channels for college users to access regarding online safety concerns, including internal, local, and national support.
- Ensure that an appropriate risk assessment is undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

ICT Services will:

- Ensure that suitable, robust, and appropriate filtering and monitoring systems are in place and updated regularly.
- Provide technical support to the Designated Safeguarding Lead, especially in the development of appropriate online safety policies and related procedures, to allow them to take appropriate safeguarding action where required.
- Proactively manage the IT infrastructure to ensure that it is as safe as is reasonably practicable against misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Be aware of and follow the College Online Safety Policy to carry out their work effectively.
- Keep up to date with online safety technical information.

All staff have a responsibility to:

- Read and adhere to the Online Safety Policy, IT Acceptable Use Policy and any associated guidance.
- Take responsibility for the equipment they use and the data they have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site. This includes but is not limited to:
  - Modeling good practice when using technology for fulfilling their contractual duties in college, and also when using technology in their personal time for non-contractual duties in college.
  - Ensuring all digital communications between staff and students or parents/carers are professional in tone and content.
  - Following good practice when using personal social media.
- Keeping personal and professional lives separate online.
- Embed online safety education within curriculum delivery, wherever possible.

- Have an awareness of a range of online safety issues and how they may be experienced by the college's students and apprentices.
- Have an awareness that online safety is a core part of safeguarding.
- Identify online safety concerns and take appropriate action by following the college's Safeguarding Procedures, including but not limited to the immediate reporting of any suspected misuse or problem to the safeguarding team
- Supervise and monitor the use of digital technologies, mobile devices, cameras etc in lessons.
- Ensure students understand and follow the Online Safety Policy and IT Acceptable Use Policy.
- Engage in mandatory safeguarding and Prevent training.
- Be responsible for their own continuing professional development in online safety.

Students, Parents and Carers will:

- Be aware of and follow College Online Safety Policy and IT Acceptable use Policy.
- Report any concern, suspicion, abuse or misuse or access to inappropriate materials to members of college staff.
- Engage with the online safety education provided by the College.
- Take responsibility for keeping themselves and others safe online.
- In the case of parents and carers, reinforce the online safety messages provided to students in College and support the College in the use of their children's personal devices.

## Monitoring

Technology in this area evolves and changes rapidly. The college will therefore review this policy annually. The policy will also be revised following any national or local policy changes, or any changes to the technical infrastructure of the College Group.

The college will regularly monitor internet use and evaluate online safety mechanisms to ensure that the policy is consistently applied, utilising available audit tools to inform any developments.

To ensure oversight of online safety the Senior Management Team and safeguarding lead governor will be informed of online safety concerns via termly Safeguarding Committee meeting reports.

## Associated Information and Guidance

- Child Exploitation and Online Protection Command (CEOP): <https://www.ceop.police.uk/Safety-Centre/>
- Childnet: <https://www.childnet.com/>
- Internet Matters: <https://www.internetmatters.org/>

- Internet Watch Foundation (IWF): <https://www.iwf.org.uk/>
- NSPCC: Keeping Children Safe Online: <https://www.nspcc.org.uk/keeping-children-safe/online-safety/>
- Childline: <https://www.childline.org.uk/>
- UK Safer Internet Centre: <https://saferinternet.org.uk/>
- Online Safety Act 2023: <https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted>
- Prevent Duty Guidance for England and Wales: <https://www.gov.uk/government/publications/prevent-duty-guidance>
- The Prevent Duty: Safeguarding Learners Vulnerable to Radicalisation: <https://www.gov.uk/government/publications/the-prevent-duty-safeguarding-learners-vulnerable-to-radicalisation>

## Related Chesterfield College Group Policies and Documents

- Safeguarding Policy (GOV05)
- Tackling Extremism and Radicalisation Policy (GOV06)
- Anti-Bullying Policy (GOV07)
- Information Security Policy (INF01)
- IT Acceptable Use Policy (INF02)
- Data Protection Policy (INF03)
- Staff Code of Conduct (PHR19)
- Staff Disciplinary Policy (PHR20)
- Student and Apprentice Disciplinary Policy (TLA03)