The Chesterfield
College Group

Online Safety Policy

Family:	Corporate Governance and Legal Frameworks
Reference Code	GOV12
Manager Responsible:	Director of Student Experience and Wellbeing
Approval Date:	Draft – awaiting approval
Issue Date:	
Review Date:	To be reviewed annually

Impact Assessment status	In preparing the policy and procedures a full Equality Impact Assessment has been carried out, with consideration to any potential disproportionate impact it might have upon staff/students with protected characteristics as defined in the 2010 Equality Act. It is the conclusion of the Policy Group that the policy and associated procedures do not adversely impact on individuals with any of the protected characteristics.
Issue Number	1 - draft
Issue Date	Awaiting approval
Review Date	
Originator	Director of Student Experience and Wellbeing
Responsibility	Director of Student Experience and Wellbeing

Contents

Aim

The policy aims to ensure that:

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

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

1. **Content:** being exposed to illegal, inappropriate or harmful material;
2. **Contact:** being subjected to harmful online interaction with others; and
3. **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

Scope

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

The policy and its associated procedures apply to all staff, students and other College users including volunteers, external contractors, remote students, apprentices and employers where students have work placements.

The policy is a child 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 work 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 browser.

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, tablets, laptops, 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.

Students and apprentices will be supported to:

- Engage in age, curriculum and level appropriate online safety education opportunities;
- Contribute, as appropriate, to the development of online safety policies;
- 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 and others safe online;
- Seek help from a trusted adult if there is an online safety concern and support others who may be experiencing online safety issues.

Chesterfield College Group Governors and Senior Leaders, in conjunction with ICT Services, the Designated Safeguarding Lead (DSL) and Curriculum Operations Managers, have ensured that the College Group has age and ability appropriate filtering and monitoring in place to limit student's and apprentice's exposure to online risk whilst on College premises. The Senior Leadership Team will ensure that regular checks are made to confirm the effectiveness and appropriateness of the College Group's approach.

The Governors and Senior Leaders 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

Digital records of all internet access by users of College Group systems will be maintained. Staff, students, apprentices and visitors will be signposted to the IT Acceptable Use Policy on first use of College internet systems and will confirm digitally that they have read and understood the policy.

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, and blocks all sites on the Internet Watch Foundation (IWF) list. Some sites will be 'soft-blocked' and be accompanied by a warning, other sites will be 'hard-blocked'.

Staff, students, apprentices and visitors 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, 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 DSL or nominated deputy in line with the College's Safeguarding Procedures.

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 staff should adhere to the IT Acceptable Use Policy and the Staff Code of Conduct in their use of personal devices and mobile phones on College premises.

Safe and appropriate use of personal devices and mobile phones will form part of the educational approach to students and apprentices across the College Group. All students and apprentices are expected to adhere to the Student Code of Conduct and any locally issued classroom management instructions in their use of personal devices and mobile phones.

Social Media

Chesterfield College Group will control student and staff access to social media whilst using College Group provided devices and systems on-site. Access to social media platforms is universally blocked by College systems.

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 Human Resources Team. Where the concern is of a safeguarding nature a report should be made to the DSL or nominated deputy as detailed in the College's Safeguarding Policy and Procedures.

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 or their location;
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private;
- That they should not meet online friends without giving proper consideration to their personal safety and where under 18 informing a trusted adult;
- To use passwords on all social media accounts;
- To only use social media sites that are appropriate for their age and ability;
- How to block unwanted communications; and
- How to report concerns to both the College and external agencies.

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

- Student Code of Conduct;
- Anti-Bullying Policy;
- Safeguarding Policy.

Organisational use of social media is guided by the internal policies and procedures of the Marketing Team. All staff members should seek advice and guidance from the Marketing Team (marketing@chestefield.ac.uk) 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 will 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.

Members of staff will 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 enforcing safe search when using Google.

Teaching and Learning of Online Safety

Chesterfield College will establish and embed a progressive online safety curriculum to raise awareness of responsible internet use amongst students and apprentices by:

- Ensuring initial education regarding safe and responsible internet use occurs during student induction and within the first six weeks of each new academic year;
- Ensuring ongoing online safety education is embedded within tutorial programmes provided 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, 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 more significant access to the internet and/or technology is required and where this would ordinarily be restricted.

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 acceptable use policies 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 purposes in accordance with relevant legislation;
- Where practicable, peer education approaches will be implemented;
- Using support, such as external visitors, to complement the College Group's internal online safety education approach.

Vulnerable Learners

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

- Children in care;
- Care leavers;
- Students and apprentices with special educational needs and disabilities (SEND);
- Students and apprentices with mental health needs;
- Students and apprentices with English as an additional language (EAL);
- Students and apprentices experiencing trauma or loss.

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

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

Chesterfield College Group 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 Group will, where appropriate:

- Provide information relating to pertinent issues around online safety to the parents/carers of students under 18/those with an EHCP;
- Publish the Online Safety Policy on the College website and publicise its publication on social media channels;
- Encourage parents/carers to read the College's IT Acceptable Use Policy.

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 that:

- 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 setting, including personal use of social media, could have an impact on their professional role and reputation;

- New resources and tools will be highlighted and developed for staff to use with students and apprentices;
- The procedure to follow regarding online safety concerns affecting students, apprentices, colleagues or other members of the College Group community.

Managing Email

The College Group's email system will be managed in line with data protection legislation and other internal policies, such as the IT Acceptable Use Policy, Information Security Policy and Codes of Conduct:

- 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 Line Manager (if received by a member of staff). When safeguarding is considered to be a factor, the DSL or nominated deputy should be notified immediately.

Members of staff are encouraged to have an appropriate work/life balance when checking and responding to email, especially when communicating with students, apprentices, and parents/carers outside of normal working hours.

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

Chesterfield College Group uses a number of learning platforms and other software packages to enable the tracking of student and apprentice progression, including:

- OneFile;
- Virtual Learning Environment (VLE);
- ProMonitor eILP;
- Tribal EBS suite of education business systems.

The College Group 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 members of staff and students/apprentices will have access to learning platforms. Accounts are disabled once a member of staff or student/apprentice 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 Group issued devices (not their personal mobile phone or another personal device) to access systems that record and store student and apprentice personal details, attainment and other digital data;
- Devices that are used 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

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

We 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 Group's systems and networks.

All members of the College Group community are made aware of our expectations regarding safe and appropriate online behaviour and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the College Group community.

Responding to Online Concerns

All responses to concerns raised will be managed within the provisions set out within the College's Safeguarding Policy and/or Anti-Bullying Policy. Concerns may include:

- Student or apprentice welfare;
- Online sexual violence and/or sexual harassment between children;
- Youth produced sexual imagery;
- Online child sexual abuse and exploitation;
- Indecent images of children;
- Cyberbullying;
- Online hate.

Implementation

The Strategic and Designated Safeguarding Leads (SSL and DSL) have lead responsibility for safeguarding and child protection, including online safety. However, all members of the College Group community have an important role to play with regards to online safety.

The DSL will:

- Act as a named point of contact for all online safety issues;
- Work alongside deputy DSLs to ensure online safety is recognised as part of the College Group's safeguarding responsibilities and that a coordinated approach is implemented;
- Ensure that all members of staff access regular, up-to-date and appropriate safeguarding training which includes online risks;
- Access regular and appropriate training and support around the additional online safety risks faced by students and apprentices with 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 Board via safeguarding reporting;
- Meet regularly (termly) with the governor with lead responsibility for safeguarding.

The Senior Management Team and Senior Leadership Team 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 SSL, DSL and any deputies by ensuring that they have sufficient time and resources to fulfil their online safety responsibilities;
- Ensure that there are robust reporting channels for the College community 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 DSL and Senior Leaders, especially in the development of appropriate online safety policies and procedures, and to allow them to take appropriate safeguarding action where required;
- Proactively manage the IT infrastructure to ensure that this is as safe as is reasonably practicable against misuse or malicious attack, whilst allowing learning opportunities to be maximised.

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;
- 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;
- Identify online safety concerns and take appropriate action by following the College's Safeguarding Procedures.

Monitoring

Technology in this area evolves and changes rapidly. Chesterfield College Group will review this policy at least annually. This policy will also be revised following any national or local policy requirements, any child protection concern or any changes to the technical infrastructure of the College Group.

Chesterfield College Group will regularly monitor internet use and evaluate online safety mechanisms to ensure that the policy is consistently applied.

To ensure oversight of online safety the Senior Management Team and Governors will be informed of online safety concerns via termly Safeguarding Board meetings. The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.

Associated Information and Guidance

- Child Exploitation and Online Protection Command (CEOP): www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- NSPCC:
  - www.nspcc.org.uk/onlinesafety
  - www.net-aware.org.uk
- Childline: www.childline.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

Related Chesterfield College Group Policies and Documents

This policy is linked to several other policies, procedures and practices:

- Safeguarding Policy (GOV05)
- Safeguarding Procedures (GOV05P)
- Tackling Extremism and Radicalisation Policy (GOV06)
- Anti-Bullying Policy (GOV07)
- Information Security Policy (INF01)
- IT Acceptable Use Policy (INF02)
- Data Protection Policy (INF03)
- Student Code of Conduct
- Staff Code of Conduct (PHR19)
- Staff Disciplinary Policy (PHR20)
- Student/Apprentice Disciplinary Policy (TLA03)
- Maintaining Professional Relationships with Students (Guidance)