****

*Motivate, Develop, Inspire*

**E-SAFETY POLICY**

**Aims:**

This policy applies to all staff, volunteers and students and anyone involved in our Federation’s activities. Its purpose is to:

● ensure the safety and wellbeing of our students/ young people is paramount when adults or students are using the internet, social media or mobile devices

● provide staff and volunteers with the overarching principles that guide our approach to online safety

● ensure that, as a Federation, we operate in line with our values and within the law in terms of how we use online devices. It sits alongside, and should be read in conjunction with, all of our Safeguarding Policies, including our; Prevent Policy which protects students from radicalisation, Anti-Bullying & Harassment Policy, and of course our Safeguarding and Student Protection Policy.

**1. Introduction**

 Being online is an integral part of students and young people’s lives. Social media, online games, websites and apps can be accessed through mobile phones, computers, laptops and tablets – all of which form a part of the lives of our students.

 The internet and online technology provide new opportunities for student learning and growth, but it can also expose them to many forms of risk. The use of technology has become a significant component of many safeguarding issues. Student sexual exploitation; radicalisation; sexual predation; ‘cyber’-bullying: technology often provides the platform that facilitates harm. An effective approach to online safety empowers us, and families, to protect and educate our young people, and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate. More importantly, educating and empowering young people from an early age, building resilience and skills against online vulnerability, is more effective than monitoring and filtering later on.

 The breadth of issues classified within online safety in terms of types of risk, mechanisms for educating, and systems for support, is quite considerable and our leaders in our Federation use resources beyond the scope of this policy. Therefore, this policy cannot cover all aspects of online safety but endeavours to outline our guiding principles of educating and supporting our students against online vulnerabilities.

 In regards to risk, these can be categorised into three areas:

 ● content (what a student can see and receive online): being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

 ● contact (when contact has been made with a student online): being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as student or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

 ● conduct (when a student interacts online by posting or uploading information): personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

 ● commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your students or staff are at risk, please report it to the AntiPhishing Working Group (https://apwg.org/ and inform a member of the leadership team)

 Online safety falls into our normal safeguarding procedures of reporting concerns and supporting students in dealing with any issue that may harm them or affect their well-being in any way. All staff at our Federation take this responsibility seriously and we have adopted a ‘whole-site’ approach to online safety.

1.1 The Board of Trustees of the Victoria College has adopted this policy to help the college meet its responsibilities for safeguarding and educating students, for regulating the conduct of employees and for complying with legislation covering the use of information and communication technologies and digital and mobile devices.

1.2 This policy was first adopted by the school’s governing body on the 3 March 2016 when the college was established and will be reviewed annually in the light of guidance from the local authority/DfE or earlier if the local authority/DfE issues further guidance in the light of particular circumstances or developments in information and communication technology.

1.3 This Policy is based on the latest Birmingham City Council E-safety Policy for Schools and the DfE guidance Teaching Online Safety in Schools January 2023

1.4 This policy should be read in conjunction with the following policies:

* Behaviour
* Data Protection/GDPR
* Safeguarding
* Code of Conduct for Support Staff
* Code of Conduct for Teaching staff
* KCSIE 2023
* Prevent risk assessment and action plan

**2. Basic principles**

2.1 In adopting this policy the governing body has taken into account the expectation by Ofsted that rigorous e-safety policies and procedures are in place in the college, written in plain English, with contributions from the whole college, updated regularly and ratified by trustees.

2.2 The policy applies to all members of the Federation’s community, including college and college staff, students, volunteers, parents and carers, governors, trustees, visitors and community users who have access to, and are users of, the Federation’s information and communication technology systems or who use their personal devices in relation to their work at the college.

2.3 The Board of Trustees expects the Executive Head Teacher and Head of College to ensure that this policy is implemented, that training in e-safety is given high priority in college and across the Federation, that consultations on the details of the arrangements for e-safety continue with all employees on a regular basis, and that any necessary amendments to this policy are submitted to this Board of Trustees for approval.

2.4 The principal context for this policy is the need to safeguard students. It will be applied in conjunction with the procedure for safeguarding everyone. It will also be applied in conjunction with the college’s safeguarding policy, behaviour and anti-bullying policies for students and with the rules and procedures governing the conduct of employees.

2.5 The Board of Trustees expects the Head of College to arrange for this policy to be published to all employees and volunteers in the college and for the school’s policy to be published across the Federation and for necessary instructions and guidance, particularly on acceptable use, to be given to students in a manner suited to their ages and abilities.

**3. Roles and responsibilities**

 **Board of Trustees**

3.1 The Board of Trustees will consider and ratify this e-safety policy, and review it annually in the light of guidance from the local authority/DfE, or sooner if the local authority/DfE issues new guidance in the light of particular circumstances or developments in information and communication technology. Trustees are expected to follow the policy in the same way as volunteers are expected to follow it, including participating in annual e-safety training if they use information and communication technology in their capacity as trustees.

3.2 Trustees are responsible for ensuring that proper procurement procedures are used if they decide to purchase information technology services from an external contractor and that City Council or other reputable specialist advice is taken on the specification for those services to ensure proper security and safeguarding of adults.

 **Executive Head Teacher**

3.3 The Executive Head Teacher is responsible for ensuring that:

* the Board of trustees is offered appropriate support to enable this policy and its application to be reviewed regularly, and to ensure that other Federation/College policies, including that on students’ behaviour, take account of this e-safety policy;
* the board of trustees is given necessary advice on securing appropriate information and communication technology systems;
* the Federation/College obtains and follows City Council or other reputable guidance on information and communication technology to support this policy;
* the Federation/college have a designated senior person/ people to co-ordinate e-safety and that these people have adequate support from, and provide support to, other employees, particularly the designated senior person for safeguarding;
* there is effective consultation with all employees, and other users of college’s information and communication technology systems, to take account of the particular features of those systems and educational, technical and administrative needs;
* the Federation/college provides all employees with training in e-safety relevant to their roles and responsibilities and that training is also provided to volunteers and trustees who use information and communication technology in their capacity as volunteers or trustees, as the case may be;
* where appropriate students are taught e-safety as an essential part of the curriculum;
* the senior leadership teams are aware of the procedures to be followed in the event of a serious e-safety incident, including an allegation made against an employee, and that all employees know to whom they should report suspected misuse or a problem ;
* records are kept of all e-safety incidents and that these are reported to the senior leadership team;
* necessary steps have been taken to protect the technical infrastructure and meet technical requirements of the college’s information and communication technology systems;
* there is appropriate supervision of, and support for, technical staff;
* access to the Server room and administrator passwords are restricted
* Any outside contractor which manages information technology for the Federation/college undertakes all the safety measures which would otherwise be the responsibility of the individual setting to the standard required by the Federation/college and is fully aware of this policy and that any deficiencies are reported to the body which commissioned the contract.

**Other employees**

3.4 Other employees are responsible for:

* + undertaking such responsibilities as have been delegated by the Executive Head Teacher commensurate with their salary grade and job descriptions;
	+ participating in training in e-safety provided by the Federation/College and in consultations about this policy and about its application, including e-safety within the curriculum;
	+ using information and communication technology in accordance with this policy and the training provided;
	+ reporting any suspected misuse or problem to the person designated by the relevant college/college for this purpose.

**Students**

3.5 Students are expected to use information and communication technology systems and devices as they have been taught and in accordance with the behaviour policy and the instructions given to them by staff.

 **Other users**

3.6 Volunteers, including trustees, who help in the college and who use information and communication technology systems and devices in helping the college are expected to

* + participate in training in e-safety provided by the Federation/College and in consultations about this policy and about its application, including e-safety within the curriculum;
	+ use information and communication technology in accordance with this policy and the training provided;
	+ report any suspected misuse or problem to the person designated by the Federation for this purpose.

**Parents**

3.7 Parents/carers who help in any of the settings as volunteers are covered by 3.6 above. Parents/carers who are not voluntary helpers are nonetheless subject to the law in the event of misuse of information and communication technology.

**4. Acceptable use**

4.1 The use of information and communication technology should follow the following general principles:

* + This policy should apply whether systems are being used on or off college/college premises.
	+ The Federation’s information and communication technology systems are intended primarily for educational use and for management and administration. During work breaks appropriate, reasonable personal use is permitted.
	+ The General Data Protection Regulation (GDPR) legislation must be followed.
	+ Users must not try to use systems for any illegal purposes or materials.
	+ Users should communicate with others in a professional manner.
	+ Users must not disclose their password and they should not write it down or store it where it is possible that another person might steal it. Users must not attempt to use another person’s user-name or password.
	+ Users must report as soon as possible any apparently illegal, inappropriate or harmful material or event to the person designated by the setting.

4.2 Employees, volunteers and governors should:

* + not open, copy, remove or alter any other user’s files without that person’s express permission;
	+ only take and/or publish images of other people with their permission, or, in the case of students, the permission of their parents or guardians;
	+ when recording or publishing such images for educational purposes should not attach to those images any names or other personal information enabling identification;
	+ as far as possible communicate with student and parents only through official communication systems and not publish personal contact details through those systems;
	+ if they occupy a senior post in which they need to keep e-mail and other messages confidential, they should request a separate e-mail address for this purpose;
	+ if they use personal devices during their work (subject to the agreement of the setting in the case of employees), ensure that the systems which they use are secure, protected with passwords and encrypted;
	+ not use personal social networking sites through the Federation’s information and communication technology systems;
	+ not open any hyperlinks in, or attachments to, e-mails, unless the source is known and trusted;
	+ ensure that their data is backed-up regularly in accordance with the rules of the Federation’s systems;
	+ only download or upload large quantities of information if they have permission to do so, in order to avoid overloading the individual college’s systems;
	+ not try to install any programmes or alter any computer settings unless this is allowed under the rules for the particular information and communication technology systems;
	+ not deliberately disable or damage any information and communication technology equipment;
	+ report any damage or faults to the appropriate member of staff.

4.3 Use of social media networks or sites, whether by students or employees, should be subject to the same standards as the Federation would expect for behaviour and conduct generally (as set out in the code of conduct for support staff and the Teachers’ Standards for teachers). The Federation accepts the separation of private life and work and will not concern itself with people’s private lives unless it appears that the law has been broken, or that an employee is in breach of contract, or that the Federation is, or will be, brought into disrepute.

Social Networking

 Whilst the internet is used by students for education purposes, away from lessons and school, some may engage in some form of social networking, i.e. “the use of dedicated websites and applications to interact with other users, or to find people with similar interests to one's own”. Apps such as WhatsApp, Tik-Tok, Instagram and Snapchat are of common use to young people. All of these have age restrictions, e.g. WhatsApp 16yrs and most others 13yrs, but in reality, many students under this age access these online systems, which can make them vulnerable to grooming, cyber-bullying, radicalisation and other dangers.

 Whilst students can be vulnerable to the approaches of others, i.e. ‘contact’, and what they see, i.e. ‘content’, it is in the risk area of ‘conduct’ where most issues arise in interaction with others. Behaviours such as posting and sharing inappropriate images of themselves and/or others including ‘sexting’, and commenting negatively on others can cause issues for students

**5. Education and training**

5.1 Education and training in e-safety will be given high priority across the Federation.

5.2 The education of students in e-safety is an essential part of each setting’s e-safety provision and will be included in all parts of the curriculum.

Teaching Online Safety

 Alongside ensuring our online safety arrangements are robust, it’s essential that we teach students about staying safe online – both in and outside of school (UK Council for Child Internet Safety).

 We speak to our students about the benefits and dangers of the internet and create an open environment for students to ask questions and raise any concerns. We continually work to embed key messages about staying safe online throughout our curriculum and ensure that students in all year groups are taught online safety skills. As with all aspects of our whole school curriculum, our ‘online-safety teaching curriculum’ is differentiated for all our students at an appropriate level to ensure they understand how to keep themselves safe online.

 Areas such as radicalisation, grooming and bullying are covered in line with relevant policies including how each of these dangers can be increased through online activity. Students are educated on how to not only protect themselves from online dangers, but also to ensure that they themselves do not become active in any negative online behaviours such as cyberbullying which can affect others.

 We deliver our online safety ‘curriculum’ in a variety of methods across our schools, such as:

 ● In lessons where internet use is pre-planned, including IT/Computing lessons

 ● Where students are allowed to freely search the internet, e.g., using search engines

 ● It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Federated IT Support Team can temporarily remove those sites from the filtered list for the period of the study.

 ● In RPSHE curriculum/lessons and guest speakers

5.3 The college will offer education and information to parents, carers and community users of the Federation about e-safety.

 Online Safety at home – advice for parents/carers

 Families play a crucial role in ensuring that their child understands the need to use the internet/mobile devices in an appropriate way. Many families may not fully understand the issues and may be less experienced in the use of ICT than their child. We will endeavour to support our families where we can by signposting resources where necessary and ensuring we have a comprehensive curriculum and actions in place to help. In addition, school events such as parents’ evenings etc. are used to offer more advice and guidance. Specific sessions on online safety can also be available when relevant.

 In today’s world, access to the internet is extremely easy and many students may have their own mobile phones. This makes the monitoring of internet use quite difficult for families, which is why educating students on the dangers is always our first priority. However, there are some steps that families can take, which may be age dependent, such as:

 ● Educate themselves about social media

 ● Discuss with their child the dangers and consequences of social media

 ● Maintain an open dialogue with their child

 ● Set guidelines and rules with their child when first allowed to use social media

 ● Establish age limits for their child, in line with those set by operators and companies

 ● Explain the importance of privacy settings with their child and check them if relevant

 ● Keep the computer in a common area of the house

 ● Encourage them to never accept a ‘friend’s request’ from people they don’t know

 ● Explain importance of keeping passwords safe

 ● Encourage them to think before they post anything in an emotional reaction to something they have seen online

Lots of advice and guidance is available online for families, including from the UK Safer Internet Centre

5.4 Suitable training will be provided through the Federation for all employees, as part of induction and subsequently during their employment in the college. There will be a regular review of the training needs of all staff and the content of training should be kept up to date. The training will be linked to training about child protection and the protection of data. It will cover related matters such as the law on copyright of electronic materials.

5.5 Volunteers and governors who use information and communication technology during their work will be offered the same training as employees.

 **Staff Training**

 **All our staff undergo safeguarding training at regular intervals as well as at induction. Included in this training is online safety. This training is delivered in a variety of methods, including in- college activities, attendance to external training, and of course participation in online training.**

 **Our Designated Safeguarding Lead directs this training alongside other members of our Senior Leadership Team to ensure we have full coverage. Our Federation governors and trustees also engage in safeguarding training. This includes knowledge of filtering and monitoring processes for the college.**

 **In addition, our staff are governed by our ‘Acceptable Use Policy’ which covers all use of internet and ICT facilities for work purposes but also gives advice and guidance on personal use of the internet, e.g. Social Networking sites, which will safeguard staff and ensure neither staff nor students are placed at unnecessary risk.**

**6. Password Security**

6.1 All staff and some children within the Federation understand the importance of keeping passwords secure from others. We recommend to all staff to use a different password for accessing organisational systems to those used for personal purposes.

If a computer workstation is left it should be left in locked mode (using Ctrl+Alt+Delete,)

**6. General Data Protection Regulation**

6.1 The Federation will ensure that its information and communication technology systems are used in compliance with current data protection legislation and are compliant with the GDPR and that all users are made aware of the data protection policy, including the requirement for secure storage of information.

8. **Technical aspects of e-safety**

8.1 The Federation will seek to ensure that the information and communication technology systems which it uses are as safe and secure as is reasonably possible by taking reputable advice and guidance on the technical requirements for those systems.

8.2 The Federation will undertake regular reviews of the safety and security of its information and communication technology systems. The college is working towards Cyber essentials plus. This includes updating of systems, certification and training.

8.3 Particular attention will be paid to secure password protection and encryption for devices located in each setting and mobile devices.

8.4 Across the Federation we subscribe to RMSafetyNet to provide the filtering of internet access for all users, preventing access to illegal content, and with additional filtering for different groups of users for inappropriate content. This also enables us to block or unblock sites ourselves as appropriate. This allows for incidents to be identified with the aim to protect people being drawn into terrorism in line with the Prevent Duty, however, it also allows for research in a safe way for educational purposes and training.

8.5 Across the Federation we also subscribe to Smoothwall,this allows us to monitor computer access across the college. They also report any incidents to us via a weekly report.

8.5 The Federation will ensure that its information and communication technology systems include standard, automated monitoring for illegal materials, profanity, and unsolicited materials (generally known as ‘spam’). It should safeguard children and adults against inappropriate use. It should provide the head teacher and senior leadership team with regular reports to indicate whether or not there have been any incidents.

8.6 Additional monitoring may take place as part of an investigation following evidence of apparent misuse.

 Filtering and Monitoring

 The Department for Education’s statutory guidance on Keeping Children Safe in Education, states that “it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such, governing bodies, trustees and proprietors should ensure appropriate filters and appropriate monitoring systems are in place.” However, we also have to ensure that over blocking does not lead to unreasonable restrictions as to what our students can be taught with regards to online teaching and safeguarding.

 We have in place strict and high-level standards in this aspect of safeguarding which is regularly checked and reported on and in line with guidance and requirement of all schools and colleges.

 It is important to recognise however, that no filtering systems can be 100% effective and needs to be supported with good teaching and learning practice and effective supervision. Smoothwall provide weekly reports to the senior leadership team and DSL on site. This identifies the number of positive ‘captures’ across the users, devices and software used and will create a level of risk (5-point scale) for each. The SLT on site will act on any positive reports that are generated and submit anonymised data to the Governing Body/trustees on a termly basis. This will be used to inform discussions around frequency and steps that have been taken to prevent future situations from occurring.

 Where appropriate, students are issued with passwords to access our IT systems in school and are instructed to keep this confidential. We also have rules on the use of mobile devices in our Federation which all students have to follow. As well as the disruption to teaching and learning, these rules are in place to safeguard students against possible online issues, at least while in our setting. Staff sign an ‘Acceptable Use Policy’ which covers staff use of technologies both inside and outside college.

9. **Dealing with incidents**

9.1 Any suspicions of misuse or inappropriate activity related to child/young person protection should be reported as prescribed in the Safeguarding Board’s protection procedures.

9.2 Any suspicions of other illegal activity should be reported to the head of/college or the Executive Head teacher, who should take advice from appropriate persons (according to the nature of the suspected activity and the individuals apparently involved) and, depending on the advice and the outcome of preliminary investigations, should report alleged criminal activity to the police and may also instigate disciplinary procedures.

9.3 Suspicions of inappropriate, as distinct from illegal, use of information and communication technology should be reported to the head teacher or other designated member of the senior leadership team for investigation and appropriate action. This may lead to informal management discussions, improved training or, depending on the nature of the alleged misuse, investigation under the disciplinary procedure for employees, or the college’s behaviour policy for students.

 Responding to concerns

Responding to concerns in this area falls into line with our normal safeguarding reporting procedures. When any staff become concerned regarding any issue, they report to our DSL and/or a member of our Senior Leadership Team, dependent on immediate availability and context of concern. An assessment of the risk is then made and appropriate actions taken. If it is concerning content/activities which are deemed illegal, then we report to the police. If it is concerning material which has bypassed our filtering system, we ensure we block any further similar material coming from the same source. In addition, dependent on actions of any students, we deal with any disregard of appropriate behaviour in our normal way using our behaviour policy; ensuring all the time that we continue and support the development of all our students.

Legislation & Guidance

 This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect students in England and has been written in consultation and reference to many sources of good practice and guidance such as;

● Keeping Children Safe in Education (updated annually)

● NSPCC E-Safety for schools ● UK Safer Internet Centre Online Safety Policy

● DfE Teaching Online Safety in school (See ‘Information and Support’ section for further documentation)

Information and Support

There is a wealth of information available to support schools, colleges and parents to keep students safe online.

UKCIS has recently published its Education for a connected world framework, which aims to support the development of the curriculum and is of particular relevance to PSHE education and Computing. It is designed to be usable across the curriculum and beyond and to be central to a whole school approach to safeguarding and online safety. It covers early years through to age 18.

As well as those resources already noted in this policy, the following list, taken from KCSiE, should provide a useful starting point for readers to extend knowledge and build up resources and advice

| organisation/Resource | What it does/provides |
| --- | --- |
| http://www.thinkuknow.co.uk/ | NCA CEOPs advice on online safety |
| https://www.disrespectnobody.co.uk/relationship-abuse/what-is-relationship-abuse/ | Home Office advice on healthy relationships, including sexting and pornography |
| http://www.saferinternet.org.uk/ | Contains a specialist helpline for UK schools and colleges  |
| http://www.swgfl.org.uk/ | Includes a template for setting out online safety policies  |
| https://www.internetmatters.org/?gclid=EAIaIQobChMIktuA5LWK2wIVRYXVCh2afg2aEAAYASAAEgIJ5vD\_BwE | Help for parents on how to keep their children safe online |
| https://parentzone.org.uk/ | Help for parents on how to keep their children safe online |
| https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation | A briefing note for schools on how social media is used to encourage travel to Syria and Iraq  |
| Harmful Online Challenges & Online Hoaxes  | https://www.gov.uk/government/publications/harmful-onlinechallenges-and-online-hoaxes/harmful-online-challenges-andonline-hoaxe |

Date Accepted by Board of Trustees: September 28th 2023
Signed

Chair of Trustees John Rodway

Review Date: September 2024