Stephen Perse

Foundation

Online Safety Policy

This policy is applicable to all the schools of the Stephen Perse Foundation (the **School**) including those pupils in the Early Years Foundation Stage (**EYFS**).

Contents

1. About this policy

At the School we have a strong pedagogical philosophy of linking digital learning to our students' curriculum to help enhance and develop learning as well as ensuring we are helping to prepare our students for the current world that they are living in. We aim to support our students in becoming flexible, fluid learners who are happy and confident to adapt to future changes. We are aware that raising the profile of digital learning in our schools means that we must have a robust strategic plan which ensures that our students are able to experience all that is on offer within a safe, structured environment.

This policy sets out the School's safety expectations of staff, parents and students, with respect to the use of the Internet, messaging systems and related technologies provided by the School, and to all school users accessing these services within the School and from home.

This policy is designed to express the School's philosophy and vision with regard to the Internet and digital communication in general. It aims to set general principles users should apply when using the services at the School, but this guidance cannot and does not attempt to cover every possible situation.

2. Review Procedure

There shall be ongoing opportunities for staff to discuss with the Designated Safeguarding Lead (**DSL**) and/or Deputy Designated Safeguarding Leads (**DDSLs**) any issue of online safety that concerns them.

The policy shall be amended if new technologies are adopted or there are changes in the regulations or guidance in any way.

This policy has been read, amended and approved by Heads of Schools, the Principal and Governors.

It has been agreed by the Senior Leadership Teams (**SLT**) (1-11 and 11-18), the Operational and Educational Executive (**OpEd**) and the Governors, that the policy shall be reviewed every year and/or after any serious incident. Any incident will be recorded in our e-safety incident logs held centrally in each school.

3. Introduction to online safety

Digital Learning (**ICT**) is seen as an essential resource to support teaching and learning within school, as well as playing a role in the everyday lives of our students. The School needs to build in the use of these technologies to prepare our young people with the skills to access lifelong learning and employment. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.

Whilst exciting and beneficial, both in and out of the context of education, much digital learning, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At the School**,** we understand the responsibility to educate our staff, parents and students about online safety issues; informing all stakeholders about the most up to date guidance available through staff training, parent workshops and for students, through assemblies and the PSHEE and Computer Science curricula. Staff training occurs within the INSET timetable, and includes a focus on online elements of child-on-child abuse and cyberbullying, as well as consensual and non-consensual relationships on social media and ongoing review of threats to online safety, as linked to the Safeguarding Policies and Technology Acceptable Use Policies.

This policy and the Technology Acceptable Use Policies (for all staff, governors, visitors and students) are inclusive of both fixed and mobile Internet technologies on devices provided by the School, and any personal device of this nature that is used or can be used for work purposes.

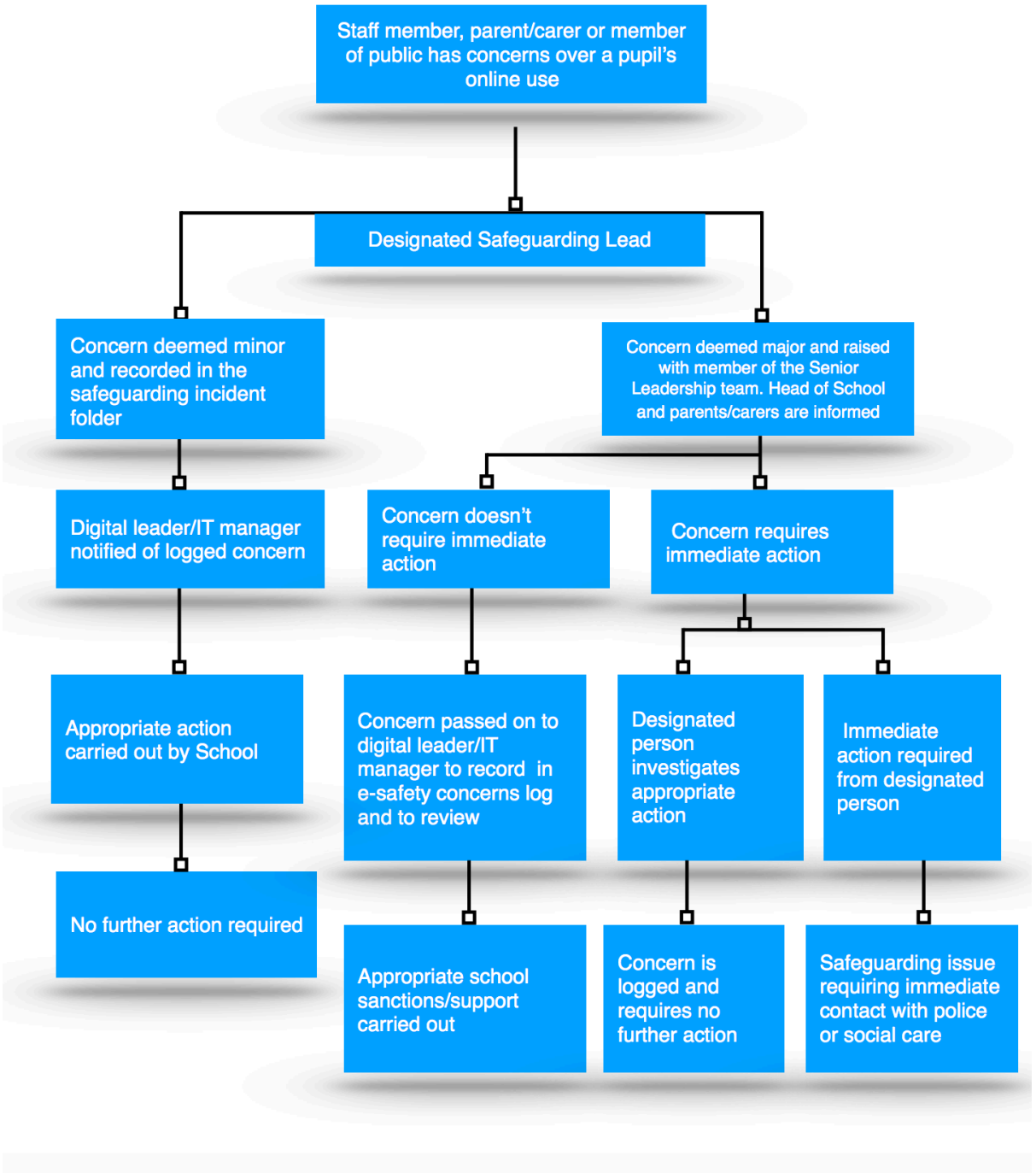
4. Roles and responsibilities

The Principal and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The name and contact details for the DSL and the DDSL for each school can be found in the Safeguarding and Child Protection Policy which is published on our website.

All members of the School community have been made aware of who the DSL and the DDSLs are. Any online safety concerns will be logged through the School's safeguarding reporting system and they will be actioned as necessary.

The School has appointed a DDSL to be the Online Safety Lead and the relevant DDSL has completed appropriate training to assist them in this role.

Flowchart showing action to be taken in the event of concerns over a student's online use



It is the role of the SLTs to ensure that all staff members at the School are kept abreast of current issues relating to e-safety, with guidance through organisations such as Cambridgeshire LEA, Essex LEA, CEOP Command (Child Exploitation and Online Protection), ThinkUKnow and Childnet.

OpEd and Governors are updated by the Safeguarding Leads and all Governors have an understanding of the issues and strategies at the School in relation to local and national guidelines and advice.

This policy, supported by the School's Technology Acceptable Use Policies which can be found here:

- Technology Acceptable Use Policies

protects the interests and safety of the whole School community. It supports the following mandatory School policies: Safeguarding and Child Protection, Health and Safety, Behaviour, Rewards and Sanctions, Anti-Bullying as well as PSHEE and Relationships and Sex Education in the curriculum and the home-school agreements.

The School's responsibility
As stated earlier, online safety covers a wider scope than just the Internet. The School includes the following in the Online Safety Policy:

- The School runs PSHEE sessions for students, educating them about the opportunities and dangers of using the Internet, empowering them to make the right decisions to keep themselves safe online.

- The DSL and DDSLs can request and access support and advice from outside agencies such as the relevant local Children's Safeguarding Board and where necessary, the Police.

- The School shall update the Online Safety Policy as required and review the policy annually to ensure that it is current and considers any emerging technologies.

- The School's Director of IT shall consult with the DSL and where appropriate the Heads of School to audit the School's filtering systems to ensure that inappropriate website categories are blocked.

- The School will ensure that students and staff are adhering to the policy, by logging any incidents of possible misuse, and ensuring that these are investigated, where appropriate, by a member of the relevant SLT, the DSL or DDSL or the Police.

- The School shall consider online safety whenever members of its community are using the Internet and ensure that every student has been educated about safe and responsible use.

- Students and staff need to know how to minimise online risks and how to report a problem, if in school or at home.

- All staff shall agree and sign the Technology Acceptable Use Policy.

- Parents of children who attend the Junior School or Dame Bradbury's shall sign and return the relevant Technology Acceptable Use Policy on behalf of their child. Senior School students either sign themselves, or have a parent sign on their behalf. Sixth Form students shall sign and return the Technology Acceptable Use Policy themselves.

Implementation

No policy can protect students without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences. Online safety awareness is an essential element of all staff and volunteer induction. Training is therefore delivered to cover the following points:

- Students should be reminded of their responsibilities whenever they are using the Internet, both in terms of the Technology Acceptable Use Policy, in navigating social media and the internet generally safely themselves, and in how to recognise and report cyberbullying and child-on-child abuse directed at themselves or others.
- Ensuring all staff, students and parents know how to report an incident of concern regarding Internet use, as well as what specific concerns may look like in a digital context.
- A member of the relevant SLT approves the School's web filtering configuration.

Measures Taken

The following is a list of technical measures taken by the School to ensure safety online.

<u>Appropriate Filtering and Monitoring</u>

There is a multi-layered approach to online safety in regards to web filtering. There is broad blocking based on website categories categorised by the firewall, application level blocking, and more granularly using keyword and url filters. The website categories that we block are based on the latest Keeping Children Safe in Education (**KCSIE 2023**) guidance, which recommends settings based on guidance from the UK Safer Internet Centre. Where students require more focused learning, we operate a web filter that only allows access to approved websites. Only essential ports and services are made available to staff and students.

Pupils in Kindergarten to Year 5 in the 3-11 environment are closely supervised and do not have access to devices without a member of staff present. Pupils in Year 6, with a 1:1 iPad, should not be using their iPad between lessons. All teachers are able to monitor school-managed mobile tablet devices in the classroom, which allows them to view screens and lock devices.

<u>Reporting and alerting</u>

All online activity that goes through the School systems is logged. Reports of web activity are sent at regular intervals to the appropriate DDSL. The reports contain a vast amount of information and detail so it is not feasible for all activity to be checked. However, if there is a particular concern or issue raised about a student, their web activity (using the reports as reference) and email history will be analysed. Random spot checks of users in the reports may be done for safeguarding and pedagogical reasons.

In order to actively identify “at risk” students whilst at school, realtime email alerting has been set up. This means that if students search for a particular keyword, the Head of Year, DSL or appropriate DDSL will be alerted via email. They will then be able to assess whether further investigation is required. They will be able to use the web activity reports mentioned above as a reference to check for any further online behaviour that is cause for concern. Due to the high volume of alerts, it is not feasible to expect an immediate response to them. For devices that are set to use the filtering systems outside of school, activity is logged and regularly reviewed, but not always actively monitored, outside of hours on school days or during holidays.

Filtering and Monitoring Offsite

Filtering and monitoring applies even when devices are off School premises, to ensure the safety of our students wherever they are connected. In the unlikely event access to the School’s filtering system fails, the device will have unrestricted web access outside of School. Parents always have the option to enable additional security measures that they control outside of school hours; this information is given to parents when their child joins the School, however, should this have been missed, please contact the appropriate school for more information.

NB. Students using a School device in the same household as another at the same time may experience incorrect filtering due to network address translation being unavailable outside of School. Parents with more than one child in the School who have a concern about this should contact the School so that the different options available can be explained.

Further measures

Further measures have been taken to ensure online safety at School. All student issued devices are managed and controlled by the School’s IT Department, and are restricted so only approved apps can be installed. In 11-18, these apps are approved by the Head of Innovative Learning in conjunction with Heads of Department, the Data Manager and the SENCO, and approved lists for each year group and individual students with SEND needs are reviewed annually. In 3-11 the apps are approved by the Head of School and the Data Manager.

Responsibilities and Expectations of Staff

Information technologies are developing rapidly and can leave staff unsure of best practice or how to discuss online safety issues with students. Advice and training for staff shall be incorporated into Child Protection Training which all staff must complete during their induction to the school and every 3 years. All staff must be signed off to state that they have attended this training.

There will be additional online safety training provided through twilight training sessions run after school and on INSET days. New and relevant information, which needs to be brought to the attention of all staff immediately, will also be incorporated into safeguarding briefings (issued when new legislation, serious case reviews or in response to in-house issues), our own Daily News and in staff briefings.

All staff shall sign a Technology Acceptable Use Policy for Staff on appointment and re-sign a new policy if any significant amendments are made. Staff know and accept that the School can monitor network and Internet use to help ensure staff and student safety.

The IT Department is responsible for the web filtering on all School devices whilst onsite.

If a member of staff suspects a student of viewing or using inappropriate or illegal content, it must be reported to the DSL or DDSL. Staff must be aware of dangers to themselves in managing ICT use; for instance, if staff view inappropriate images to investigate their source, this needs to be reported to the DSL or DDSL immediately.

In the event of a concern about or allegation of inappropriate behaviour by staff, the procedures set out in the Safeguarding and Child Protection Policy or Low Level Concerns policy (as appropriate) will be followed. Advice should be sought from the DSL and / or Cambridgeshire or Essex Police.

Digital communications provide additional channels for staff, parents and students to communicate. Inappropriate behaviour can occur and communications can be misinterpreted. When sending parents or students an email, staff must only use the School's mailing systems. Staff must not give out their own personal contact details, and must never send or accept texts or images that could be viewed as inappropriate. If a member of staff receives content that is offensive in any way they need to notify the DSL or DDSL so that the matter can be investigated further. Contact with students and parents must be through School devices and systems only.

In limited circumstances, it may be appropriate for staff to use a personal mobile phone for work purposes. Where possible this should always be agreed with a DSL or a member of OpEd in advance. Such circumstances include:

- Emergency evacuations
- Parental contact in an emergency (mobile phones setting that allow for the number not to be identified should be used)
- When participating in School trips or visits

It is essential that staff do not accept students or parents as friends or "follow" them on social media sites – until there is no longer any professional responsibility (i.e. when the student has left the School). Consideration should be given to the age of the student at the time of leaving and caution exercised even when there is no professional responsibility. Staff and students must ensure their personal social media accounts do not negatively risk the reputation of themselves or the School and suitable privacy settings are applied where necessary. Creating School social media accounts requires approval from either the Marketing and Communications Manager or a member of the relevant SLT.

Staff and students should exercise extreme caution in online messaging and forum and chat environments where it is impossible to determine the age, identity or potential motives of individuals. The advice would be to not engage in discussions or conversations where this is the case. Staff should also refer to the School's Code of Conduct for all Staff Working With Young People.

Staff should be aware that students may be subject to child-on-child abuse, or cyberbullying via electronic methods of communication both in and out of school. If a student informs staff that this is happening, staff have an obligation to report this to the Head of Year of the student, and/or the DSL/DDSL. Staff must not investigate an issue themselves, or ask a student to investigate. Staff have received training on the updated KCSIE 2023 and the processes by which concerns around online

safety should be brought to the attention of the DSL and addressed in order to protect the students involved, themselves, and any other relevant stakeholders.

The Principal, and staff authorised by the Principal (which includes Heads of School, the Head of Boarding, a member of the SLT and Heads of Year or Heads of Phase), have a statutory power to search a student or their possessions and confiscate items such as mobile phones in certain situations. The Searching and Retention and Disposal of Confiscated Items policy must be followed in such circumstances.

Protection of School accounts and data is vital. Reference should be made to the Technology Acceptable Use policy for staff and Data Protection Policy for further information.

Authorised images taken of students using a School device shall be removed from it and stored securely on School systems, and not kept longer than necessary. Staff need to take particular care with sharing features to make sure images are not synced or shared to other unsecured or unauthorised devices or persons. Location settings should be appropriately configured to keep the location of staff and students private.

5. Laws to be aware of that relate to e-safety Legal Framework

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and changes occur frequently. Please note this section is designed to inform users of legal issues relevant to the use of communications, it is not professional advice.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003
Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as “Sexting”). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as

videos, photos or webcams. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, counsellors etc. fall in this category of trust). Any sexual intercourse with a child under the age of 16 commits the offence of rape.

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 2018
The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 - 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences against or in another country.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This can include racist, xenophobic and homophobic comments, messages etc.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using the author's "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited

purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 - 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006, it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he/she knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him/her is guilty of an offence if he/she knows or ought to know that his/her course of conduct will cause the other so to fear on each of those occasions. This also includes incidents of racism, xenophobia and homophobia.

Regulation of Investigatory Powers Act 2000
The Regulation of Investigatory Powers Act 2000 (**RIP**) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008
Section 63 makes it an offence to possess an "extreme pornographic image". This includes "explicit and realistic" images of an act which "threatens a person's life, … results or is likely to result in serious injury to a person's anus, breasts or genitals, … involves sexual interference with a human corpse" or a person performing a sexual act on "an animal (whether alive or dead)" (section 63(7)). Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006
The Education and Inspections Act 2006 outlines legal powers for schools which relate to cyberbullying/bullying.

Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of students off site.

School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the School behaviour/anti-bullying policies.

Keeping Children Safe in Education (KCSIE 2023)
This is statutory guidance from the Department for Education (the **DfE**) issued under Section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014, and the Non-Maintained Special Schools (England) Regulations 2015. Schools and colleges in England must have regard to it when carrying out their duties to safeguard and promote the welfare of children.

Related Policies

- Anti-Bullying Policy
- Behaviour Rewards and Sanctions Policy
- Child-on Child Abuse Policy
- Code of Conduct for All Staff Working with Young People
- Data Protection Policy
- Low Level Concerns Policy
- PSHEE Policy
- Risk Assessment Policy for Student Welfare
- RSE Policy
- Safeguarding and Child Protection Policy
- Searching and Retention and Disposal of Confiscated Items Policy
- Technology Acceptable Use Policies
- AI Policy

Reviewed: March 2024

Version Control

Date of adoption of this policy	15 April 2024
Date of last review of this policy	March 2024
Date for next review of this policy	Autumn Term 2024
Policy owner	Designated Safeguarding Lead (DSL)
Authorised by	The Governing Body