JEP YOUTH ENGAGEMENT

ONLINE SAFETY POLICY

Policy Name: Online Safety

Policy Reference: OS - E

Version: 002

Date: 19 June 2024

Next Review Date: September 2026

Author: Senior Management

Owner: Levi Wolfenden

Revision History:

Revision No.	Date	Summary of changes	Reviewer
1	20/11/2025	PUPILS/CHILDREN TO YOUNG PEOPLE	L. Wolfenden
2		CYBER-BULLYING	
3		THE 4 KEY CATEGORIES OF RISK	
4		THE DESIGNATED SAFEGUARDING LEAD (DSL/DDSLs)	
5		Artificial intelligence (AI)	
6		STAFF USING WORK DEVICES OUTSIDE OF JEP	
7		ACCEPTABLE USE OF THE INTERNET AT JEP	

AIMS

JEP Youth Engagement aims to:

- Have robust processes in place to ensure the online safety of young people, staff and volunteers
- Identify and support groups of young people that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole provision community in its use of technology including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

THE 4 KEY CATEGORIES OF RISK

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as young people with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Young people Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for head teachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting young people from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

ROLES AND RESPONSIBILITIES

The Non-Executive Director has overall responsibility for monitoring this policy and holding the CEO to account for its implementation.

The Non-Executive Director will:

- make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
- make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard young people.
- co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
- ensure young people are taught how to keep themselves and others safe, including keeping safe online.
- ensure the provision has appropriate filtering and monitoring systems in place on devices and networks and will regularly review their effectiveness. The Education SLT will review the DfE filtering and monitoring standards, and discuss with In4Tech and service providers what needs to be done to support JEP in meeting the standards, which include:
    - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
    - Reviewing filtering and monitoring provisions at least annually.
    - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.
    - Having effective monitoring strategies in place that meet their safeguarding needs.

The Non-Executive Director will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of JEP's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable young people, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all young people in all situations, and a more personalised or contextualised approach may often be more suitable.

THE FOUNDER/CEO

The CEO/Founder is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout their provision.

THE DESIGNATED SAFEGUARDING LEAD (DSL)

Details of the DSLs and DDSLs are set out below:

Role	Name
CEO/Director	Jamie Pilling
Designated safeguarding lead (DSL)	Jason Whittaker (Secondary) Levi Wolfenden (Primary) Gary Smith (My Futures Programme)
Deputy DSLs	Chloe Radcliffe, Ian Joslin, Ben Sharples, Adam Worrall (Secondary) Jack McQuade, Jenny Convey, Charlotte Glynn (Primary)

The Designated Safeguarding Lead (DSL) takes lead responsibility for online safety, in particular:

- Supporting the provision leads in ensuring that staff understand this policy and that it is being implemented consistently throughout their school
- Working with the Education SLT and the CEO to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with In4Tech to make sure the appropriate systems and processes are in place
- Working with the provision leads, In4Tech and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the provision's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety to the provision leads, CEO and Non-Executive Director as required
- Undertaking annual risk assessments that consider and reflect the risks young people face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

ALL STAFF AND VOLUNTEERS

All staff, including contractors and volunteers, are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of JEP's ICT systems and the internet and ensuring that young people follow the JEP's terms on acceptable use

- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting this to the DSL
- Following the correct procedures by contacting JEP's ICT provider if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged using CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

PARENTS/CARERS

Parents/carers are expected to:

- Notify a member of staff or provision leads of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of JEP's ICT systems and internet during the induction process

Parents can seek further guidance in keeping young people safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

VISITORS AND MEMBERS OF THE COMMUNITY

Visitors and members of the community who use any of JEP's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

EDUCATING YOUNG PEOPLE ABOUT ONLINE SAFETY

Young people will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education. (For teaching until 31 August 2026)

All schools must teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

Young people in **Key Stage (KS) 1** will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Young people in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour

- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

Young people in **Key Stage (KS) 3 & 4** will be taught to:

- An online / E-safety / cyber bullying lesson is delivered every half term to re-fresh and solidify learning among the students.
- All students are monitored and observed when they are on the laptops during lessons.
- All laptops are equipped with cyber security blocks so areas such as online networking and any words that are deemed inappropriate or of risk are blocked and a message is sent to SLT
- Regular conversations are had in subjects such as Personal development and ICT regarding the dangers of online activity.
- posters are clearly visible in the ICT regarding dangers.

Many of our young people are only with us for short periods of time therefore we will endeavour to cover as much of the curriculum as possible during their stay with us, however not all young people will access all the content. The home school holds the ultimate responsibility for full curriculum coverage.

The safe use of social media and the internet will also be covered in other subjects where relevant.
We will raise each young person's awareness of the dangers that can be encountered online through things such as life skills sessions, personal development and guest speakers.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable young people, victims of abuse and some pupils with SEND.

EDUCATING PARENTS/CARERS ABOUT ONLINE SAFETY

JEP will raise parents' awareness of internet safety in letters or other communications home, the induction process and in information via our website. This policy will also be available on our website for parents to access.

JEP will let parents know:

- What systems JEP uses to filter and monitor online use (see acceptable use of ICT policy)
- What their young people are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concern in relation to online safety, these should be raised in the first instance with the provision leads and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff, the CEO or Non-Executive Director.

CYBER-BULLYING

a) Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy)

b) Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that young people understand what it is and what to do if they become aware of it happening to them or others. We will ensure that each young person knows how to report any incidents and is encouraged to do so, including where they are a witness rather than the victim.

Each provision will actively discuss cyber-bullying with their cohort, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers and learning support mentors will

discuss cyber-bullying with young people during the curriculum and enrichment activities as and when appropriate.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways of supporting young people, as part of safeguarding training.

Information on cyber-bullying for parents will be available on the website so that they are aware of the signs, how to report it and how they can support young people who may be affected.

In relation to a specific incident of cyber-bullying, each provision will follow the processes set out in the provision's behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, each provision will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

c) Examining electronic devices

The provision leads, and specific staff authorised to do so by the CEO, can carry out a search with permission from the young person and home school and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or young people, and/or
- Is identified in JEP's rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is and consider the risk to other young people and staff. If the search is not urgent, they will seek advice from the provision leads and/or the DSL
- Explain to the young person why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the young person's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or

- The young person and/or the parent/carer refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with young people and young people

Any search of young people will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour and safeguarding policy

Any complaints about searching for or deleting inappropriate images or files on a young person's electronic device will be dealt with through JEP's complaints procedure.

d) Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, young people and parents/carers may be familiar with generative chatbots such as ChatGPT.

JEP recognises that AI has many uses to help young people learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

JEP will treat any use of AI to bully pupils very seriously, in line with our anti bullying and behaviour policy.

Staff should be aware of the risks of using AI tools while they are still being developed and where new AI tools are being used by JEP, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, young people and staff.

ACCEPTABLE USE OF THE INTERNET AT JEP

All young people, parents/carers, staff and volunteers are expected to sign an agreement regarding the acceptable use of the JEP's ICT systems and the internet. Visitors will be expected to read and agree to JEP's terms on acceptable use if relevant.

Use of JEP's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements and the acceptable use of ICT policy.

YOUNG PEOPLE USING MOBILE DEVICES AT JEP

Young people may bring mobile devices into school for use on transport only. All devices are to be handed to a staff member on arrival, in line with the mobile phone policy.

STAFF USING WORK DEVICES OUTSIDE OF JEP

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use.
If staff have any concerns over the security of their device, they must seek advice from the ICT provider.

HOW JEP WILL RESPOND TO ISSUES OF MISSUSE

Where a young person misuses the JEP's ICT systems or internet, we will follow the procedures set out in our policies on Acceptable Use of ICT and Social Media Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses JEP's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff handbook. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

JEP will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

TRAINING

a) Staff

All new staff members will receive training, as part of their induction, in safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). They will also complete specific online safety training every 2 years.

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that young people are at risk of online abuse
- Young people can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse

- Develop the ability to ensure young people can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence young people to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually.

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

b) Young people

All young people will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Young people will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

LINKS WITH OTHER POLICIES

- Employee Handbook (Staff Code of Conduct)
- Health and Safety Policy
- Equality, Diversity and Inclusion Policy
- GDPR Policy
- Confidentiality Policy
- Safeguarding Policies
- Social Media policy