DOCUMENT	reviewed	By whom?
Online Safety Policy	22/09/2025	Leon Edwards

Next review date - on or before	15/09/2026
Managing Director Primary Director Student Welfare – Secondary Senior Provision Practitioner – Primary	Leon Edwards Lyndsey Edwards Daisy Knock Kay Hard
Contact details	leon@pushforward.uk
	0330 818 0186

Purpose of this Policy

Pushforward, works with some of the most valuable young people who rely on the use of the internet and technology to support their needs and communicate with the outside world. Therefore, we deem balance and education overarching principles of our policy. We understand that computing covers a wide range of activities, including access to information, electronic communications and social networking. As use of technology is now universal, young people need to learn computing skills to prepare themselves for the working environment and it is important that the inherent risks are not used to reduce young people use of technology. Further, the educational advantages of computing need to be harnessed to enhance young people learning.

The purpose of this policy statement is to:

• ensure the safety and wellbeing of young people is paramount when adults, young people 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 an organisation, we operate in line with our values and within the law in terms of how we use online devices.

Legal framework

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping young people Safe in Education and also refers to the DfE'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 cyberbullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so

The association risks for young people are broken to two for areas and are defined within Keeping Children Safe in Education 2023. These are summarised below:

Content

The internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for children. There is a danger that young people may be exposed to inappropriate images such as pornography, or information advocating violence, racism, suicide or illegal and anti-social behaviour that they are unable to evaluate in a critical manner.

Contact

Chat rooms, gaming sites and other social networking sites can pose a real risk to young people as users can take on an alias rather than their real names and can hide their true identity. The sites may be used by adults who pose as Young People in order to befriend and gain children's trust (known as "grooming") with a view to sexually abusing them. Young people may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also in advertently put other young people at risk by posting personal information and photographs without consent. The internet may also be used as a way of bullying a child or for child-on-child abuse.

Commerce

Young people are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences, such as fraud or identity theft, for themselves and their parents. They may give out financial information, for example, their parent's credit card details, in response to offers for goods or services without seeing the fraudulent intent. Contact via social networking sites can also be used to persuade Young people to reveal computer passwords or other information about the family for the purposes of fraud.

Culture

Young people need to be taught to use the internet in a responsible way, as they may put themselves at risk by:

becoming involved in inappropriate, anti-social or illegal activities because of viewing unsuitable materials or contact with inappropriate people

using information from the internet in a way that breaches copyright laws uploading personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience

online bullying and child on child abuse (use of mobile devices for the purposes of sexual harassment such as the consensual and non-consensual taking and distributing of inappropriate images of the young person (sexting) that cannot be removed from the internet and can be forwarded on to a much wider audience than the child intended.

Young people may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development and their educational attainment. They may visit sites that advocate extreme and dangerous behaviour such as self-harm or suicide or violent extremism, and more vulnerable

Young People may be at a high degree of risk from such sites. All young people may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these on-line.

Educating online safety

Pushforward will:

- Offer bespoke education to suit individuals to understanding how to keep themselves safe online and how to challenge others
- Educate young people on British Values and how they relate in everyday life
- Create secure relationships between adults and young people where they feel it is safe to share concerns
- Display safer internet guidance in all sites
- Appoint an online safety lead

Acceptable Use Policy

All students, staff, volunteers are expected to adhere to the acceptable use of ICT systems and the internet. Use of the internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. Pushforward will monitor the websites visited by students, staff, volunteers to ensure they comply with the above. More information is set out in the acceptable use agreements in Appendix A.

Use of Wi-Fi

All Pushforward site have accessible Wi-Fi which are password protected. Staff are not to share this password with anyone including students unless it forms part of a student safety plan. Any breaches in this will result in new passwords being created.

Mobile Phone use

Staff Mobiles

All staff are issued with company mobile phone that are monitored by IT. These mobile phones are preloaded with apps that are deemed necessary for the job role. All phones have pin numbers and can be tracked remotely. Students are only given access to staff phones where full supervision is present, for educational purposes such as using geo cache app or taking pictures.

Staff are required to carry a second mobile phone (a personal phone) for emergency use only. Students should have no access to these phones and staff should not be using personal phones during the delivery session.

Students Mobiles

Some students particularly in secondary and post 16 will bring a mobile phone to sessions. The use of students using their mobile phone will be discouraged. Students within primary will be encouraged to hand over their phone on arrival for safe keeping. Students should not be left alone with personal mobile phones and staff should screen anything that they wish to share with peers before allowing this.

Using company issue devices for learning

Pushforward value the use of technology in supporting the learning of its students. All staff are issued with company issue laptops. These laptops can be used for learning but only with direct supervision of staff. They should not be given to students for independent study where content cannot be monitored. Staff should use websites for learning such as BBC bitesize, Twinkl, Kids you tube to limit risk of exposure to inappropriate content.

Using devices away from company locations

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 are at least 8 characters, with a combination of upper and lower-case letters
- 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 of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates
- Staff members must not use the device in any way which would violate the Pushforwards terms of acceptable use
- Work devices must be used solely for work activities.

- If staff have any concerns over the security of their device, they must seek advice from the Head Office

Artificial intelligence

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, and students may be familiar with generative chatbots such as ChatGPT and Google Bard. The New Wave Federation recognises that AI has many uses to help pupils 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. Staff should be aware of the risks of using AI tools whilst they are still being developed. Staff are to seek permission to use AI for teaching and learning purposes from SLT. Should a decision be made to use it, then staff members should carry out a risk assessment where new AI tools are being used.

Searching of devices

Any member of SLT, can carry out a search of and confiscate any electronic device that they have identified through the monitoring and filtering procedure that;

- Poses a risk to staff or students,
- and/or is evidence in relation to an offence

SLT have a statutory power to search a pupil or their possessions where they have reasonable grounds to suspect that the pupil may have a prohibited item that the member of staff reasonably suspects has been, or is likely to be used to commit an offence (Searching, Screening and Confiscation - GOV.UK).

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

- Make an assessment of how urgent the search is, and consider the risk to other student and staff.
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the students cooperation 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 DSL 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 if 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 student and/or the parent 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 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 children and young people
Any searching of pupils 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
Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the complaints procedure.

Responding to issues of misuse
Pushforward's will take all incidents of misuse by staff or young people seriously. Depending on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
This may include but will not be limited to:

- Sanction around the use of technology during sessions
- Education on staying safe online
- Staff disciplinary procedures
- In incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.
- Respond in accordance with out Safeguarding policy
- Record and monitor all incidents for repeated pattens

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