



## Alternative Provision Service

(Encompassing the 3 PRU Bases, Launchpad Tuition, and Launchpad Alternative)

### E-Safety Policy

#### Vision

To provide a high quality, personalised educational experience that meets learners' needs and leads to success for all.

#### Mission

A positive and inclusive community where young people are encouraged to achieve high standards of progress and succeed in a supported, safe environment.

#### Our Values / Principles

Individuals Aspirations Raised  
New Experiences  
Safety and Support  
Personalised Programmes  
Individuals Feeling Valued  
Respect  
Excellence in Learning

|                            |                          |                         |
|----------------------------|--------------------------|-------------------------|
| <b>Approved by:</b>        | PRU Management Committee | <b>Date:</b> 14/07/2021 |
| <b>Last reviewed on:</b>   | 09/11/2019               |                         |
| <b>Next review due by:</b> | July 2022                |                         |

## **Policy Aims**

## **Policy Scope**

Links with other policies

## **Monitoring and Review**

## **Roles and Responsibilities**

Headteacher and Governing Body  
Designated Safeguarding Lead (DSL)  
Staff Members  
Pupils  
Parents/Carers

## **Education and Engagement Approaches**

Education and Engagement with Pupils  
Vulnerable Pupils  
Training and Engagement with Staff  
Awareness and Engagement with Parents/Carers

## **Reducing Online Risks**

## **Safer Use of Technology**

Classroom Use  
Managing Internet Access  
Filtering and Monitoring  
Decision Making  
Filtering  
Monitoring  
Managing Personal Data Online  
Security and Management of Information Systems  
Password Policy  
Managing the Safety of Our Network  
Publishing Images and Videos Online  
Managing Email  
Staff Email  
Educational Use of Videoconferencing and/or Webcams  
Users  
Content  
Management of Learning Platforms  
Management of Applications (apps) Used to Record Pupils' Progress

## **Social Media**

Expectations  
Staff Personal Use of Social Media  
Pupils' Personal Use of Social Media  
Official Use of Social Media

## **Use of Personal Devices and Mobile Phones**

Expectations  
Staff Use of Personal Devices and Mobile Phones  
Pupils' Use of Personal Devices and Mobile Phones  
Officially Provided Mobile Phones and Devices

## **Responding to e-Safety Incidents and Concerns**

- Concern about Pupils' Welfare
- Staff Misuse

## **Procedures for Responding to Specific Online Incidents or Concerns**

- Online Sexual Violence and Sexual Harassment between Pupils
- Youth Produced Sexual Imagery
- Online Sexual Abuse and Exploitation (Including Criminal Exploitation)
- Indecent Images of Children (IIOC)
- Cyberbullying
- Online Hate
- Online Radicalisation and Extremism

## **e-Safety Links and Contacts**

## POLICY AIMS

This e-Safety policy has been written by PACE and Launchpad, involving staff, pupils and parents/carers, building on the St Helens Council IT guidelines, with specialist advice and input as required.

It takes into account the DfE statutory guidance '[Keeping Children Safe in Education](#)' 2020, '[Working Together to Safeguard Children 2018](#)' and the St Helens Safeguarding procedures.

The purpose of PACE and Launchpad's e-Safety policy is to:

- Safeguard and protect all members of PACE and Launchpad community online
- Identify approaches to educate and raise awareness of e-Safety throughout the community
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to e-Safety concerns

PACE and Launchpad identifies that the issues classified within e-Safety are considerable, but can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

## POLICY SCOPE

PACE and Launchpad believes that e-Safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.

PACE and Launchpad identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.

PACE and Launchpad believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of PACE and Launchpad (collectively referred to as "staff" in this policy) as well as pupils, parents/carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets or mobile phones.

### **Links with other policies:**

This policy links with several other policies, practices and action plans including:

- Anti-bullying policy
- Behaviour Policy
- Child Protection Policy for Managing Allegations Against Staff
- Confidentiality Policy
- Curriculum Policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data Protection Policy
- Safeguarding Policy
- Staff Disciplinary Policy

## **MONITORING AND REVIEW**

Technology in this area evolves and changes rapidly. PACE and Launchpad will review this policy at least every two years.

The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.

We will regularly monitor internet use and evaluate e-Safety mechanisms to ensure that this policy is consistently applied.

To ensure they have oversight of e-Safety, the Designated Safeguarding Lead, will be informed of e-Safety concerns, as appropriate.

The named governor for safeguarding will report on a regular basis to the Governing Body on e-Safety practice and incidents, including outcomes.

Any issues identified via monitoring will be incorporated into our action planning.

## **ROLES AND RESPONSIBILITIES**

The Designated Safeguarding Lead (DSL) has lead responsibility for e-Safety. Whilst activities of the DSL may be delegated to other appropriately trained staff, overall the ultimate lead responsibility for safeguarding and child protection, including e-Safety remains with the DSL.

PACE and Launchpad recognises that all members of the community have important roles and responsibilities to play with regards to e-Safety.

### **Headteacher and Governing Body**

The Headteacher and Governing Body will:

- ensure that e-Safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements
- ensure there are appropriate and up-to-date policies regarding e-Safety; including a Behaviour Policy, which covers acceptable use of technology
- ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks
- ensure that e-Safety is embedded within a progressive curriculum, which enables all pupils to develop an age-appropriate understanding of e-Safety
- support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their e-Safety responsibilities
- ensure there are robust reporting channels for the community to access regarding e-Safety concerns, including internal, local and national support
- ensure that appropriate risk assessments are undertaken regarding the safe use of technology
- audit and evaluate e-Safety practice to identify strengths and areas for improvement

## **Designated Safeguarding Lead (DSL)**

The DSL will:

- act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate
- work alongside the teachers in charge of each service area to ensure e-Safety is recognised as part of PACE and Launchpad's safeguarding responsibilities and that a coordinated approach is implemented
- ensure all members of staff receive regular, up-to-date and appropriate e-Safety training
- access regular and appropriate training and support to ensure they understand the unique risks associated with e-Safety and have the relevant knowledge and up to date required to keep pupils safe online
- access regular and appropriate training and support to ensure they recognise the additional risks that pupils with SEN and disabilities (SEND) face online
- keep up-to-date with current research, legislation and trends regarding e-Safety and communicate this with the community, as appropriate
- ensure that e-Safety is promoted to parents, carers and the wider community, through a variety of channels and approaches
- maintain records of e-Safety concerns, as well as actions taken, as part of PACE and Launchpad's safeguarding recording mechanisms
- monitor e-Safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures
- report e-Safety concerns, as appropriate, to the Leadership Team and Governing Body
- work with the Leadership Team to review and update e-Safety policies on a regular basis (at least annually) with stakeholder input
- meet annually with the governor with a lead responsibility for safeguarding and online safety

## **Staff Members**

It is the responsibility of all members of staff to:

- contribute to the development of e-Safety policies
- read and adhere to the e-Safety policy and acceptable use policies
- take responsibility for the security of school systems and the data they use or have access to
- model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site
- embed e-Safety education in curriculum delivery, wherever possible
- have an awareness of a range of e-Safety issues and how they may be experienced by the pupils in their care
- identify e-Safety concerns and take appropriate action by following PACE and Launchpad's safeguarding policies and procedures
- know when and how to escalate e-Safety issues, including signposting to appropriate support, internally and externally
- take personal responsibility for professional development in this area

It is the responsibility of staff managing the technical environment to:

- provide technical support and perspective to the DSL and Leadership Team, especially in the development and implementation of appropriate e-Safety policies and procedures
- implement appropriate security measures as directed by the DSL and Leadership Team, such as password policies and encryption, to ensure that PACE and Launchpad's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised
- ensure that the filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the Leadership Team
- ensure that the monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the Leadership Team
- ensure appropriate access and technical support is given to the DSL and the Teachers in Charge to the filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required

### **Pupils**

It is the responsibility of pupils (at a level appropriate to their age and ability) to:

- engage in age appropriate e-Safety education opportunities
- contribute to the development of e-Safety policies
- read and adhere to the acceptable use policies
- respect the feelings and rights of others both on and offline
- take responsibility for keeping themselves and others safe online
- seek help from a trusted adult, if there is a concern online, and support others that may be experiencing e-Safety issues

### **Parents/Carers**

It is the responsibility of parents/carers to:

- read the acceptable use policies and encourage their children to adhere to them
- support PACE and Launchpad's e-Safety approaches by discussing e-Safety issues with their children and reinforcing appropriate and safe online behaviours at home
- role model safe and appropriate use of technology and social media
- identify changes in behaviour that could indicate that their child is at risk of harm online
- seek help and support from PACE and Launchpad, or other appropriate agencies, if they or their child encounter risk or concerns online
- contribute to the development of the e-Safety policies
- use school systems, such as learning platforms, and other network resources, safely and appropriately
- take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies



## **EDUCATION AND ENGAGEMENT APPROACHES**

### **Education and Engagement with Pupils**

PACE and Launchpad will establish and embed a progressive e-Safety curriculum to raise awareness and promote safe and responsible internet use amongst pupils by:

- ensuring education regarding safe and responsible use precedes internet access
- including e-Safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study
- reinforcing e-Safety messages whenever technology or the internet is in use
- educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation
- teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

PACE and Launchpad will support pupils to read and understand the acceptable use policies in a way which suits their age and ability by:

- displaying acceptable use posters in all rooms with internet access
- informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation
- rewarding positive use of technology
- providing e-Safety education and training as part of the transition programme across the key stages and when moving between establishments

### **Vulnerable Pupils**

PACE and Launchpad recognises that some pupils are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

PACE and Launchpad will ensure that differentiated and ability appropriate e-Safety education, access and support is provided to vulnerable pupils.

When implementing an appropriate e-Safety policy and curriculum, PACE and Launchpad will seek input from specialist staff as appropriate, including the SENCO and the Designated Teacher for Looked After and previously Looked After Children.

## **Training and Engagement with Staff**

We will:

- provide and discuss the e-Safety policy and procedures with all members of staff as part of induction
- provide up-to-date and appropriate e-Safety training for all staff on a regular basis, with at least annual updates - this will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations
- recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape e-Safety policies and procedures
- make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices
- make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation
- highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils
- ensure all members of staff are aware of the procedures to follow regarding e-Safety concerns affecting pupils, colleagues or other members of the community

## **Awareness and Engagement with Parents/Carers**

PACE and Launchpad recognises that parents/carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

We will build a partnership approach to e-Safety with parents/carers by:

- providing information and guidance on e-Safety in a variety of formats
- drawing their attention to the e-Safety Policy and expectations during induction meetings, in letters and on PACE and Launchpad's website
- requesting that they read e-Safety information as part of joining PACE and Launchpad, for example, within our home school agreement
- requiring them to read our acceptable use policies and discuss the implications with their children

## **REDUCING ONLINE RISKS**

PACE and Launchpad recognises that the internet is a constantly changing environment with new applications, devices, websites and material emerging at a rapid pace.

We will:

- regularly review the methods used to identify, assess and minimise online risks
- examine emerging technologies for educational benefit and undertake

- appropriate risk assessments before use in PACE and Launchpad is permitted
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material

Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via PACE and Launchpad's computers or devices.

All members of the community are made aware of PACE and Launchpad's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the acceptable use policies and highlighted through a variety of education and training approaches.

## **SAFER USE OF TECHNOLOGY**

### **Classroom Use**

PACE and Launchpad uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Learning platforms, such as TEAMS
- Email
- Games consoles and other games-based technologies
- Digital cameras, web cams and video cameras

All school owned devices will be used in accordance with the acceptable use policies and with appropriate safety and security measures in place.

Members of staff will always evaluate websites, tools and applications fully before use in the classroom or recommending for use at home.

We will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.

We will ensure that the use of internet-derived materials, by staff and pupils complies with copyright law and acknowledge the source of information.

Supervision of pupils will be appropriate to their age and ability.

Pupils will be appropriately supervised when using technology, according to their ability and understanding.

## **Managing Internet Access**

All staff and pupils will read and sign an acceptable use policy before being given access to our computersystem, IT resources or internet.

## **Filtering and Monitoring**

Levels of Internet access and supervision will vary according to the pupil's age and experience. Teachers may need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, the restrictions imposed by PACE and Launchpad's filtering system may be removed temporarily while the user accesses the material under close supervision but still using the Smoothwall filtering system via St Helens IT.

PACE and Launchpad will work with the local authority to ensure that systems to protect users are constantly under review.

PACE and Launchpad will apply the St Helens Council IT recommended filtering system to all Internet access.

Staff and pupils who discover that an unsuitable site is accessible must report this to PACE and Launchpad's e-SafetyCoordinator.

St Helens IT Support will manage the configuration of the filtering system to ensure that it is appropriate, effective and reasonable.

PACE and Launchpad will report any online material it believes to be illegal to the appropriate agencies.

## **Decision Making**

PACE and Launchpad's IT Support has ensured that the school has age and ability appropriate filtering and monitoring in place, to limit pupil exposure to online risks.

The IT Support is aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.

Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.

Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the Leadership Team; all changes to the filtering policy are logged and recorded.

The Leadership Team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

### **Filtering**

Education broadband connectivity is provided through St Helens IT. The Smoothwall filtering policy is continually reviewed.

Smoothwall blocks sites which can be categorised as pornography, racial hatred, extremism, gaming, gambling and sites of an illegal nature.

The filtering system blocks all sites on the [Internet Watch Foundation](#) (IWF) list.

If pupils discover unsuitable sites, they will be required to report their concern to a member of staff. The member of staff will report the concern (including the URL of the site if possible) to the DSL and /or the St Helens IT Support and the breach will be recorded and escalated as appropriate.

Parents/carers will be informed of filtering breaches involving their child.

Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Merseyside Police or Child Exploitation and Online Protection command (CEOP).

### **Monitoring**

We will appropriately monitor internet use on all school owned or provided internet enabled devices.

If a concern is identified via monitoring approaches the DSL will be informed as appropriate.

All users will be informed that use of the systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

### **Managing Personal Data Online**

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation.

Full information can be found in our Data Protection Policy.

### **Security and Management of Information Systems**

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems
- Not using portable media without specific permission; portable media will be checked by an anti-virus/malware scan before use
- Not downloading unapproved software to work devices or opening unfamiliar email attachments
- Regularly checking files held on our network
- The appropriate use of user logins and passwords to access our network
- Specific user logins and passwords will be enforced for all
- All users are expected to log off or lock their screens/devices if systems are unattended

### **Password Policy**

All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.

From Year 7, all pupils are provided with their own unique username and private passwords to access our systems; pupils are responsible for keeping their password private.

We advise/require all users to:

- Use strong passwords for access into our system
- Change their passwords regularly
- Always keep their password private; users must not share it with others or leave it where others can find it
- Not login as another user at any time

### **Managing the Safety of Our Network**

We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).

We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.

Staff or pupil's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.

### **Publishing Images and Videos Online**

We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the: Behaviour Policy, Child Protection Policy, Data Protection Policy and Safeguarding Policy.

### **Managing Email**

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies including (but not limited to) the: Behaviour Policy, Child Protection Policy, Data Protection Policy and Safeguarding Policy.

The forwarding of any chain messages/emails is not permitted.

Spam or junk mail will be blocked and reported to the email provider.

Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.

School email addresses and other official contact details will not be used for setting up personal social media accounts.

Members of the community will immediately tell the DSL and/or St Helens IT Support if they receive offensive communication, and this will be recorded in our safeguarding files/records.

Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

### **Staff Email**

The use of personal email addresses by staff for any official setting business is not permitted.

All members of staff are provided with an email address to use for all official communication.

Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, pupils and parents.

### **Educational Use of Videoconferencing and/or Webcams**

PACE and Launchpad recognise that videoconferencing and the use of webcams can be a challenging activity but brings a wide range of learning benefits.

All videoconferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.

### **Users**

Parents/carers consent will be obtained prior to pupils taking part in videoconferencing activities.

Videoconferencing will be supervised appropriately, by recording the TEAMS lesson.

Only teachers will be given access to videoconferencing administration areas, this has been disabled for students.

Teachers should be made clear to students at the start of the lesson that the TEAMS lesson will be recorded.

### **Management of Applications (Apps) Used to Record Pupils' Progress**

Launchpad uses ePraise to track pupils' progress and share appropriate information with parents/carers.

To safeguard pupils' data:

- personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store pupils' personal details, attainment or images unless appropriately encrypted
- devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft
- all users will be advised regarding safety measures, such as using strong passwords and logging out of systems
- parents/carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords



## **SOCIAL MEDIA**

### **Expectations**

The expectations regarding safe and responsible use of social media applies to all members of PACE and Launchpad community.

The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

All members of PACE and Launchpad are expected to engage in social media in a positive, safe and responsible manner.

All members of PACE and Launchpad are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

We will control pupil and staff access to social media whilst using school provided devices and systems on site.

Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.

Concerns regarding the online conduct of any member of PACE and Launchpad community on social media, should be reported to the DSL and will be managed in accordance with our Child Protection Policy for Managing Allegations against Staff, Anti-bullying, Behaviour and Safeguarding Policies.

### **Staff Personal Use of Social Media**

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policies.

### **Reputation**

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within PACE and Launchpad.

Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites.

Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Being aware of location sharing services
- Ensuring staff do not represent their personal views as that of PACE and Launchpad
- Keeping passwords safe and confidential
- Logging out of accounts after use
- Opting out of public listings on social networking sites
- Setting the privacy levels of their personal sites

Members of staff are encouraged not to identify themselves as employees of PACE and Launchpad on their personal social networking accounts; this is to prevent information on these sites from being linked with the school, and to safeguard the privacy of staff members.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with our policies and the wider professional and legal framework.

Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.

Members of staff will notify the DSL and/or the Headteacher immediately if they consider that any content shared on social media sites conflicts with their role.

#### Communicating with pupils and parents/carers

All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or their family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this, will be discussed with the DSL and/or the Headteacher.

If ongoing contact with pupils is required once they have left PACE and Launchpad, members of staff will be expected to use official setting provided communication tools.

Staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the DSL and/or the Headteacher.

Any communication from pupils and parents received on personal social media accounts will be reported to the DSL and/or The Headteacher.

### **Pupils' Personal Use of Social Media**

Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.

Any concerns regarding a pupil's use of social media will be dealt with in accordance with existing policies, including anti-bullying, behaviour and safeguarding. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

Pupils will be advised:

- How to block and report unwanted communications
- How to report concerns both within the setting and externally
- Not to meet any online friends without a parent/carer or other responsible adult's permission and
  - only when a trusted adult is present
- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private
- To use safe passwords
- To use social media sites which are appropriate for their age and abilities

## **USE OF PERSONAL DEVICES AND MOBILE PHONES**

PACE and Launchpad recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within the school.

### **Expectations**

All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as Anti-bullying, Behaviour and Child Protection and Safeguarding.

Electronic devices of any kind that are brought onto site are the responsibility of the user.

All members of PACE and Launchpad community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.

Students will hand in their mobile devices at the start of the school day which will be stored securely and handed back for use during break and lunchtime.

All members of PACE and Launchpad community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.

All members of PACE and Launchpad community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our Behaviour, Safeguarding or Child protection Policies.

### **Staff Use of Personal Devices and Mobile Phones**

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: Data Protection, Safeguarding and Child Protection Policy for Managing Allegations against Staff.

Staff will be advised to:

- Ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations
- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times
- Keep mobile phones and personal devices in a safe and secure place during lesson time
- Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times
- Not use personal devices during teaching periods, unless permission has been given by the Headteacher, such as in emergency circumstances

Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents/carers. Any pre-existing relationships, which could undermine this, will be discussed with the DSL.

Staff will not use personal devices:

- to take photos or videos of pupils unless permission has been given by the Headteacher, and will only use work-provided equipment for this purpose
- directly with pupils and will only use work-provided equipment during lessons/educational activities

If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour policy.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

### **Pupils' Use of Personal Devices and Mobile Phones**

Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

Mobile phones and personal devices must not be taken into examinations. Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

## **Officially Provided Mobile Phones and Devices**

Members of staff will be issued with a work phone number and email address, where contact with pupils or parents/carers is required. In addition, occasionally school provided mobile phones/devices will be issued to staff where appropriate.

School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.

School mobile phones and devices will always be used in accordance with the relevant policies.

## **RESPONDING TO E-SAFETY INCIDENTS AND CONCERNS**

All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns. Pupils, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

We require staff, parents/carers and pupils to work in partnership to resolve online safety issues. After any investigations are completed, the DSL will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

If we are unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.

Where there is suspicion that illegal activity has taken place, the DSL will contact the Education Safeguarding Team or Merseyside Police using 101, or 999 if there is immediate danger or risk of harm.

If an incident or concern needs to be passed beyond our community (for example if other local schools are involved or the public may be at risk), the DSL will speak with Merseyside Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

## **Concerns about Pupils' Welfare**

The DSL will be informed of any online safety incidents involving Safeguarding or Child Protection concerns. The DSL will record these issues in line with our Safeguarding and Child Protection policies.

The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the St Helens Safeguarding Children Board thresholds and procedures.

The DSL and/or DCPC will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

## **Staff Misuse**

Any complaint about staff misuse will be referred to the DSL and/or the St Helens IT Support.

Any allegations regarding a member of staff's online conduct will be discussed with the Local Authority Designated Officer (LADO).

Appropriate action will be taken in accordance with our Child Protection Policy for Managing Allegations against Staff, Behaviour, Safeguarding policies.

# **PROCEDURES FOR RESPONDING TO SPECIFIC ONLINE INCIDENTS OR CONCERNS**

## **Online Sexual Violence and Sexual Harassment Between Children**

Our school has accessed and understood '[Sexual violence and sexual harassment between children in schools and colleges](#)' (2018) guidance and part 5 of '[Keeping Children Safe in Education](#)' 2018.

PACE and Launchpad recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation. Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our Behaviour, Child Protection and Anti-bullying Policies.

PACE and Launchpad recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

PACE and Launchpad also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

PACE and Launchpad will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE curriculum.

We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.

We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of online sexual violence and sexual harassment, we will:

- Immediately notify the DSL and act in accordance with our Behaviour, Child Protection and Anti-bullying Policies
- If content is contained on pupils' electronic devices, they will be managed in accordance with the DfE ['searching screening and confiscation'](#) advice
- Provide the necessary safeguards and support for all pupils involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support
- Implement appropriate sanctions in accordance with our behaviour policy
- Inform parents/carers, if appropriate, about the incident and how it is being managed
- If appropriate, make a referral to partner agencies, such as Children's Social Services and/or the Police
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community
- If a criminal offence has been committed, the DSL will discuss this with Merseyside Police first to ensure that investigations are not compromised
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate

### **Youth Produced Sexual Imagery**

PACE and Launchpad recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL.

We will follow the advice as set out in the non-statutory UK Council for Child Internet Safety (UKCCIS) guidance: ['Sexting in schools and colleges: responding to incidents and safeguarding young people'](#) and St Helens Safeguarding guidance.



PACE and Launchpad will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.

We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using school provided or personal equipment.

We will not:

- view any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so - If it is deemed necessary, the image will only be viewed by the DSL and their justification for viewing the image will be clearly documented
- send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request pupils to do so

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- act in accordance with our safeguarding and child protection policies and the relevant St Helens Safeguarding procedures
- ensure the DSL responds in line with the ['Sexting in schools and colleges: responding to incidents and safeguarding young people'](#) guidance
- store the device securely
- if an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image
- inform parents/carers, if appropriate, about the incident and how it is being managed
- make a referral to Children's Social Services and/or the Police, as deemed appropriate in line with the UKCCIS : ['Sexting in schools and colleges: responding to incidents and safeguarding young people'](#) guidance
- implement appropriate sanctions in accordance with our Behaviour Policy but taking care not to further traumatise victims where possible
- consider the deletion of images in accordance with the UKCCIS: ['Sexting in schools and colleges: responding to incidents and safeguarding young people'](#) guidance
- delete images only when the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation

### **Online Sexual Abuse and Exploitation (Including Criminal Exploitation)**

PACE and Launchpad will ensure that all members of the community are aware of online child sexual abuse, including exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

PACE and Launchpad recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL.

We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for pupils, staff and parents/carers.

We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

If made aware of an incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- act in accordance with our child protection policies and the relevant St Helens Safeguarding procedures
- if appropriate, store any devices involved securely
- make a referral to Children's Social Services (if required/appropriate) and immediately inform Merseyside Police via 101, or 999 if a child is at immediate risk
- carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies)
- inform parents/carers about the incident and how it is being managed
- provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support

PACE and Launchpad will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using school provided or personal equipment.

Where possible, pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report:

[www.ceop.police.uk/safety-centre/](http://www.ceop.police.uk/safety-centre/)

If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Education Safeguarding Team and/or Merseyside Police.

If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the DSL.

If pupils at other settings are believed to have been targeted, the DSL will seek support from Merseyside Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

## **Indecent Images of Children (IIOC)**

PACE and Launchpad will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

If we are unclear if a criminal offence has been committed, the DSL will obtain advice immediately through Merseyside Police and/or the Education Safeguarding Team.

If made aware of IIOC, we will:

- act in accordance with our child protection policy and the relevant St Helens Safeguarding Child Boards procedures
- store any devices involved securely
- immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Merseyside Police or the LADO

If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children, we will:

- ensure that the DSL is informed
- ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via [www.iwf.org.uk](http://www.iwf.org.uk)
- ensure that any copies that exist of the image, for example in emails, are deleted
- report concerns, as appropriate to parents/carers

If made aware that indecent images of children have been found on PACE and Launchpad provided devices, we will:

- ensure that the DSL is informed
- ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via [www.iwf.org.uk](http://www.iwf.org.uk)
- ensure that any copies that exist of the image, for example in emails, are deleted
- inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Services (as appropriate)
- only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only
- report concerns, as appropriate to parents/carers

If made aware that a member of staff is in possession of indecent images of children on school provided devices, we will:

- ensure that the DSL and the Headteacher are informed in line with our Child Protection Policy for Managing Allegations Against Staff
- inform the LADO and other relevant organisations in accordance with our Child Protection Policy for Managing Allegations Against Staff
- quarantine any devices until police advice has been sought

### **Cyberbullying**

Cyberbullying, along with all other forms of bullying, will not be tolerated at PACE and Launchpad.

Full details of how we will respond to cyberbullying are set out in our anti-bullying and safeguarding policies.

### **Online Hate**

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at PACE and Launchpad and will be responded to in line with existing policies, including Anti-bullying and Behaviour.

All members of the community will be advised to report online hate in accordance with relevant policies and procedures.

The Police will be contacted if a criminal offence is suspected.

If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the Education Safeguarding Team and/or Merseyside Police.

### **Online Radicalisation and Extremism**

We will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site.

If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our Child Protection and Safeguarding Policies.

If we are concerned that member of staff may be at risk of radicalisation online, the DSL and the Headteacher will be informed immediately, and action will be taken in line with the Child Protection Policy for Managing Allegations against Staff and Safeguarding Policy.

## E–SAFETY LINKS AND CONTACTS

|   |  |
|---|--|
| <b>Local Authority Designated Officer (LADO) – Katherine Appleton</b>                                     | <a href="mailto:Sthelenslado@sthelens.gov.uk">Sthelenslado@sthelens.gov.uk</a><br>Tel: LADO Secretary<br>01744 671265        |
| <b>Safeguarding &amp; Pastoral Manager / Designated Safeguarding Lead / Signs of Safety Practice Lead</b> | <a href="mailto:Katherinecrook@sthelens.gov.uk">Katherinecrook@sthelens.gov.uk</a><br>Tel: Work Mobile 07748112722           |
| <b>Nominated Governor for Safeguarding – Jeanette Devine</b>  | <a href="mailto:jeanette.devine.jd@gmail.com">mailto:jeanette.devine.jd@gmail.com</a>  |
| <b>Merseyside Police</b>  | <a href="http://www.merseyside.police.uk">www.merseyside.police.uk</a><br>0151 709 6010<br>In case of an emergency dial 999  |
| <b>Child Exploitation and Online Protection (CEOP)</b>  | <a href="http://www.ceop.police.uk">www.ceop.police.uk</a><br><a href="http://www.thinkuknow.co.uk">www.thinkuknow.co.uk</a> |
| <b>Childnet</b>   | <a href="http://www.childnet.com">www.childnet.com</a>   |
| <b>NSPCC</b>  | <a href="http://www.nspcc.org.uk/onlinesafety">www.nspcc.org.uk/onlinesafety</a>   |
| <b>Childline</b>  | <a href="http://www.childline.org.uk">www.childline.org.uk</a>   |
| <b>UK Safer Internet Centre</b>   | <a href="http://www.saferinternet.org.uk">www.saferinternet.org.uk</a>   |
| <b>Internet Watch Foundation</b>  | <a href="http://www.iwf.org.uk">www.iwf.org.uk</a>   |