# PACE Academy Trust

# Online Safety (inc Social Media) Policy

## Key Contacts

| | | |
|---|---|---|
| | Designated Safeguarding Lead (DSL) team | Mrs J Stevens |
| | Online-safety lead (if different) | Mr C Andreotti<br>Mrs J Stevens |
| | Online-safety / safeguarding link governor | |
| | PSHE/RSHE lead | Mrs E Seward |
| | Network manager / other technical support | OpenAir Systems |
| | Date this policy was reviewed and by whom | Sept 2022 PACE DSL team/ZH |

# Contents

## Introduction

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2022 and other statutory documents.  it is designed to sit alongside our PACE Early Help and Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

## Aims

This policy aims to:

- Set out expectations for all PACE community members' online behaviour, attitudes and activities and use of digital technology.
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns.

## Roles and responsibilities

PACE Academy Trust and its respective schools form a community and all members have a duty to behave respectfully online and offline; to use technology for teaching and learning and to prepare for life after school; and to immediately report any concerns or inappropriate behaviour to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

## Headteacher

**Key responsibilities:**

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles

- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements

## Designated Safeguarding Lead / Online Safety Lead

**Key responsibilities**:

- "The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] … this **lead** responsibility should not be delegated" (KCSiE)
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding
- Ensure that online safety education is embedded across the curriculum
- Promote an awareness of and commitment to online safety throughout the school community
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident
- Facilitate training and advice for all staff, including supply teachers:
  - all staff must read KCSIE Part 1 and all those working with children Annex B
  - all staff must be aware of Annex D (online safety)
  - cascade knowledge of risks and opportunities throughout the organisation

## Governing Body

**Key responsibilities**

- Approve this policy and strategy and subsequently review its effectiveness
- Ensure an appropriate senior member of staff, from the school leadership team, is appointed to the role of DSL to lead responsibility for safeguarding and child protection (including online safety)
- Have regular strategic reviews with the online-safety lead / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B; check that Annex D on Online Safety reflects practice in your school
- Ensure that all staff undergo safeguarding and child protection training (including online safety)
- Ensure appropriate filters and appropriate monitoring systems are in place.
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum.

## All Staff

**Key responsibilities:**

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Read Part 1, Annex B and Annex D of Keeping Children Safe in Education
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures – **CPOMS**
- Sign and follow the staff acceptable use policy and code of conduct
- Notify the DSL if policy does not reflect practice in the school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum.
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites
- When supporting pupils remotely, be mindful of additional safeguarding considerations
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and sexual harassment
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
- Avoid any private communication with pupils

## Subject Leaders

**Key responsibilities:**

- As a Subject Leader look for opportunities to embed online safety in your subject or aspect, especially as part of the RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE/RSE and health education curriculum. This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face.
- Work closely with other leaders to avoid overlap but ensure a complementary whole-school approach

- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE and Computing

## Pupils

**Key responsibilities:**

- Read, understand, sign and adhere to the pupil acceptable use policy
- Treat home learning in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Avoid any private communication with school staff or tutors
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

## Parents/Carers

**Key responsibilities:**

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Encourage children to engage fully in home-learning and flag any concerns
- Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.

## Network Manager/Technician –OpenAir Systems

**Key responsibilities:**

- Support the HT and DSL team as they review protections for pupils in the school and remote-learning procedures, rules and safeguards
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead ensure that school systems and networks reflect school policy
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy

## Data Protection Officer (DPO)

**Key responsibilities:**

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents such as 'Keeping Children Safe in Education'
- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

## LGfL Nominated Contacts

**Key responsibilities:**

- To ensure all LGfL services are managed on behalf of the school in line with school policies, following data handling procedures as relevant
- Work closely with the DSL and DPO to ensure they understand who the nominated contacts are and what they can do / what data access they have, as well as the implications of all existing services and changes to settings that you might request.

## Volunteers (including any PTA) and Contractors

**Key responsibilities:**

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media

- Maintain an awareness of current online safety issues and guidance
- Support the school in promoting online safety and data protection

## Education and Curriculum

At PACE Academy Trust we recognise that online safety and broader digital resilience must thread throughout the curriculum

The following subjects have the clearest online safety links:

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing
- Citizenship / Wellbeing Curriculum

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Whenever overseeing the use of technology in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

All staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

## Handling Online-Safety Concerns and Incidents

It is vital that all staff recognise that online-safety is a part of safeguarding and online safety concerns must be handled in the same way as any other safeguarding concern.

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

The school will actively seek support from other agencies as needed. We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

## Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter. It is important not to treat online bullying separately to offline bullying and to recognise that much bullying will often have both online and offline element.

## Online Sexual Violence and Harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL immediately. Staff should work to foster a zero-tolerance culture. Schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate.

All schools should refer to the updated UK Council for Internet Safety (UKCIS) guidance Sharing nudes and semi-nudes: advice for education settings to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

**No staff should attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.**

## Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

## Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school; nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms

# Misuse of School Technology

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). These are defined in the relevant Code of Conduct and Acceptable Use Policies as well as in this document.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

## Social Media Incidents

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct (for staff). Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the school will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

## Data Protection and Data Security

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements.

The headteacher, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

At PACE, the internet connection is provided by LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

At PACE, we combine all three aspects of monitoring.

## Electronic communications

### Email

Email is the official electronic communication channel between parents and the school, and between staff and pupils. Teachers to Parents is used to send texts and email communication from the school to parents but not to receive them.

Staff at this school use the StaffMail system, and Teachers to Parents for all school emails. Egress is used in some cases. StaffMail and systems are linked to the USO authentication system and are fully auditable, trackable and managed by LGfL on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email, Evidence Me, Google Classroom, and Microsoft Teams are the only means of electronic communication to be used between staff and pupils / staff and parents (in both directions).
- Email may only be sent using the systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email.
  - If data needs to be shared with external agencies, USO-FX and Egress systems are available from LGfL.
  - Internally, staff should use the school network, including when working from home when remote access is available via the Connect2School, RAV3 system
- Appropriate behaviour is expected at all times. The system must never be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Pupils and staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

## Cloud Platforms

The following principles apply:

- Training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work

## Digital Images and Video

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long.

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name and photo file names/tags do not include full names to avoid accidentally sharing them

At PACE Academy Trust, no member of staff will ever use their personal phone to capture photos or videos of pupils except in the rarest of circumstances. These circumstances must always be agreed with the DSL/DPO and Headteacher, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services.

Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually and at each public performance about the importance of not sharing without permission, due to reasons of child protection and data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated and are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

## Social Media

Our school works on the principle that if we don't manage our social media reputation, someone else will. Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online. We manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Social media is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be

followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+, Tik Tok 13+), but the school regularly deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. Children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use, with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Class WhatsApp groups, maintained by members of the PTA must adhere to the remits of this policy.

Pupils are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, and should be declared upon entry of the pupil or staff member to the school.

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

## Device Usage

**Pupils** (Year 5 and 6) are allowed to bring mobile phones in for emergency use only. They are stored in the classroom and signed in and out.  Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to the withdrawal of mobile privileges.  Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies. Pupils are not allowed to wear 'wearable technology' such as apple watches as these have

camera and recording facilities. Where **home devices** are issued to some students, these are restricted to the apps/software installed by the school and may be used for learning and reasonable and appropriate personal use at home, but all usage may be tracked.

**All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.

For school trips/events away from school, teachers may be issued a school duty phone – and this number is used for any authorised or emergency communications with parents. Any deviation from this policy (e.g., by mistake or because the school phone will not work) will be notified immediately to the headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number

**Volunteers, contractors, governors** should leave their phones in their pockets/bags and set to silent mode. Under no circumstances should they be used in the presence of children or to take photographs or videos without explicit permission from the headteacher (and this should be done in the presence of a member staff).  Volunteers, contractors and governors can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.

**Parents** are asked to leave their phones in their pockets and on silent mode when they are on site. They should ask permission before taking any photos, e.g., of displays in corridors or classrooms, and avoid capturing other children. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office. Parents have no access to the school network or wireless internet on personal devices

## Searching and Confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Document Control Table

| 1. Document Control Table | |
|---|---|
| **Document Title** | Online Safety Policy |
| **Author** | Sally Dubben – Trust Designated Safeguarding Leads |
| **Version number:** | 1 |
| **Date approved:** | 8.12.22 |
| **Approved by:** | PACE Strategic Board |
| **Document History:** | |

| Version | Date | Author | Note of revisions |
|---|---|---|---|
| | | | . |