Progress Schools

E-Safety Policy

2023/2024

Policy issue and updates

Pages	***Issue No.***	***Date***
Whole Document - (Replaced Acceptable Computer and Internet Use policy and Social Networking Acceptable Use Policy).	1	December 2022
Whole document – annual review	2	August 2022
Whole document – annual review	3	August 2023

The following policy has been approved by the Managing Director and Senior Leadership Team.
The policy will be reviewed on an annual basis unless circumstances arise requiring the policy to be reviewed earlier.

Approved by Executive Team: August 2023

Board signatory: CBarton

Planned review: August 2024

1. Policy overview

1.1 We recognise that technology and the use of ICT equipment is part of everyday life and that it is an essential part of learning and employment. ICT systems are one of the fastest and most effective ways of finding information, sharing ideas, and working with other people, but whilst effective there is also the opportunity for risks to occur.

1.2 As part of our safeguarding responsibility, we aim to protect all staff and students against risks associated to the internet and other technology aids, such as mobile phones - this will be known as e-safety. The risks to users can comprise of data that is inaccurate, dangerous, illegal, and offensive. This includes exposure to and the release of extremist material and data that is considered private and confidential.

1.3 Students, staff, and any other user with Internet access must follow our codes of conduct and adhere to any signed commitment statements as well as Company handbooks and any points raised in this policy.

1.4 We ensure that the leadership team and relevant staff are aware of and understand the systems in place, manage them effectively whilst knowing how to escalate concerns when identified.

2. Risks

2.1 The risks associated with technology can be categorised under the following headings:

Physical
Including poor posture (affected by poor seating and furniture set up) and eye strain (due to the length of time a person is exposed to the screen). Progress Schools conducts annual reviews on staff Health and Safety around display screen equipment (DSE). It would be the responsibility of the staff to assess whether a student requires assistance or support around DSE.

Contact
Social networking sites, chatrooms and phone apps allow people to meet new friends but unfortunately not everyone is who they claim to be. Never give personal information out as this could make you vulnerable to: radicalisation, exploitation (sexual and criminal), bullying or sexual aggression. Never feel you need to keep new relationships a secret. A real friendship and/or new relationship would not need to be kept a secret, and there may be a hidden agenda to this, putting you at risk.

Conduct
This behaviour can be by or towards individuals and can include cyberbullying and cyberstalking. Behaviours can also include racism and piracy. When using equipment provided by us you have a right to be protected and a duty to behave honestly and responsibly. Never do anything that makes you vulnerable to malicious software or charges of bad behaviour. Incorrect use of equipment including downloading or passing on illegal or inappropriate content can result in the user committing a criminal offence. Any inappropriate act, that offends or harms others, is taken very seriously and will be reported to the Police. This is both in and outside of work/school. Never share information that is considered private and confidential.

Content
This includes downloading information, some of which may be illegal, containing extremist material and be dishonest or inappropriate. This presents risks to the employer if using their equipment. Posting personal information can also pose risks as previously mentioned in the 'contact' category.
Potential data breaches and non-following of data protection law is a big risk about the 'content' of data. This is inclusive of sharing, controlling, processing, and even holding/storing data – there needs to be a rationale for the processing, sharing, and storing of content/data – this always needs to be considered when collecting information, as does the timeframe for storage along with the security.

Commerce
This includes the risk of financial abuse when making a purchase online through an unsecure source. Always check that a site belongs to the company it says it does – if in doubt look for a real-world postal address or phone number. You will also find a padlock key in the toolbar (sometimes green), this represents a safe and secure site. If you're ever unsure, don't risk it and check with the provider.

3. Curriculum

3.1 As part of the ICT, SMSC and Wellbeing/RSE curricula, all students will undertake awareness lessons in E-Safety. This is further reinforced in all other areas of the curriculum, especially when working with technology.

The key messages from these lessons are:

- The dangers of using the internet/apps both at home and at school
- What to do if they come across inappropriate/offensive text or images
- How to stay safe when communicating online
- How to take appropriate action when things go wrong
- How to stay safe when using Social Networking sites such as Facebook, Chat Roulette etc.
- How to stay safe in chat rooms/discussion forums
- What to do if they are a victim of cyberbullying
- The dangers and laws of 'sexting' and sharing inappropriate images/videos

3.2 We operate filtering systems within our school which is designed to restrict access to inappropriate sites and sites that are not needed as part of students' education. This is monitored and reviewed regularly by SLT and proprietors as some develop ways around these safeguarding blocks. We are mindful that "over-blocking" can lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding. DSL'S understand the filtering and monitoring system and effectively monitor the strategies that meet the safeguarding requirements of the school. Governors and Proprietors review the provision annually and ensure it is effective. We also have a computer use strategy where all students are supervised when using our computers/tablets/interactive whiteboards. All induction training for staff covers expectations, roles and responsibilities for their understanding of filtering and monitoring.

3.3 The use of social networking sites is not permitted in school, on school equipment.

3.4 As an underpinning message, these are the E-Safety Golden Rules that students are educated on.

- Never arrange to meet anyone you have met on the web
- Never give out personal information e.g., telephone numbers, address, photos
- If you come across anything on the web that is inappropriate/offensive, tell an adult

- Never use your real name – always a nickname
- Keep your password a secret from others – only share passwords with parents/carers so they can support you
- If you receive a nasty message or picture, report it to an adult, block and report it to the site you are on
- Make sure that when using social networking sites, privacy settings are checked so that not just anyone can see your page/photos
- Only use a webcam with people you know and have met face to face

3.5 Staff are vigilant during use of websites/technology and will monitor for potential risks including;

- Harassment or online bullying ("cyberbullying") on the part of the student or others'
- Posting information about themselves that: a) could be used to embarrass or manipulate them; b) could cause psychological harm; c) could be used by criminals to steal their identity or property or – though very rare – determine their physical location to cause physical harm
- Damage to reputation or future prospects because of young people's own behaviour or that of their peers – unkind or angry posts, compromising photos or videos, or group conflict depicted in text and imagery
- Spending too much time online, losing a sense of balance in their activities
- Exposure to inappropriate content
- Potential for inappropriate contact with adults (parents/guardians need to ensure that social networking does not lead to offline contact unapproved by them and other caring adults in their children's lives).
- Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE) which can start on Social Media.

4. Bring your own device (BYOD)

4.1 The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning within and beyond the classroom. This can lead to students bringing in and using their own devices to provide a greater freedom of choice and usability. However, this leads to several e-safety considerations. In the first instance, we ask parents/carers to support us by not allowing devices to be brought in to school unless requested to do so.

4.2 If a student chooses to bring their electronic device to school, they must adhere to all school rules relating to such technologies. All devices must be handed in for lessons unless students are asked to use them. A breach of these rules will result in sanctions as outlined in the Behaviour and Anti-Bullying Policy.

4.3 Progress Schools accept no responsibility for devices brought onto the school premises in the case of damage, loss, or theft.

4.4 Students are not permitted to show or share inappropriate or illegal content from their own devices on school premises. This may result in their phone being confiscated and handed to the Police, as is our duty of care.

5. Use of technologies

5.1 Whether using school equipment or personal, users shall not visit internet sites, make, post, download, upload, pass on, remark or comment on content that relates to;

- Pornography (including child pornography)
- Promoting discrimination of any kind
- Promoting religious hatred
- Promoting illegal acts
- Weapons
- Display any other information that may be offensive to other students, staff, visitors, or any member of the public
- Use any other users accounts nor amend or delete any of their accounts, files, or passwords
- Install or attempt to install programmes of any type

5.2 In any instance where inappropriate content is suspected or observed, staff members are to apply the school rules as applicable. Content used to bully others will be taken very seriously as per the Behaviour and Anti-Bullying Policy.

5.3 If the material is deemed to be serious, a device may be confiscated and retained as evidence (of a criminal offence or a breach of school rules). Examples of illegal activity that may require police intervention would include.

- Child sexual abuse and images (including images of one child held by another child)

- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials
- Recordings of criminal activity as a witness (this includes child on child abuse, including 'upskirting')
- The use of weapons to injure someone

5.4 If students appear to have been 'sexting' each other or someone outside of school, staff will immediately inform the DSL and National DSL who will conduct a full investigation. This may result in internal sanctioning or referral to the Police or Children's Services if one or more party are at risk of harm.

NB – Sexting means 'sending sexually explicit messages and/or suggestive images, such as nudes. While the name suggests that this is done via text messages, these types of messages can be sent via any messaging service, including emails and social media sites/apps. It is illegal for a child aged under 18 to take a nude photo of themselves or a friend, as well as distributing them.

6. Remote learning through technology

6.1 Students working from home, or other locations, (Remote Learning) means that students are spending an increased amount of time on devices. As well as the advice outlined in this policy, staff will provide additional support to parents/carers around e-safety.

6.2 Staff will maintain professional boundaries when using remote classroom technology and continue to educate students around online etiquette and safety. Any inappropriate comments to staff online, via any social media platform will be taken very seriously as per the Behaviour and Anti-Bullying Policy. This is also the case of for any online bullying towards other pupils or child-on-child abuse that is disclosed to the school during this time.

6.3 Where staff are required to teach via an online virtual classroom, they must first seek permission of the parents/carers. A set of ground rules must be established and should include:

- The student is not to undertake the lesson from a bedroom. They must be in an open area of the family home, e.g., living room, dining room

- The student must be appropriately dressed as if they were physically attending school
- Behaviour agreed – normal classroom expectations will still apply
- If there is a need to record the session (e.g., for observational purposes, written consent must be obtained from the parent/carer

6.4 If staff wish to use a virtual classroom they must:

- Outline to the Executive Team which platform they will be using and the security attached, including data protection. Many platforms have their own terms of service. E.g., Zoom is designed for 16+ only. If you wish to use it for younger ages, you must subscribe to Zoom Education. You must ensure all terms of service are abided by
- Ensure settings are secure. E.g., only invited participants can attend, you have control of microphones and cameras to promote effective learning

6.5 Where remote classroom/face to face style learning is used, preferably this would take place with the teacher inside the school building. Where staff must work from home and need to conduct virtual lessons, the following must be adhered to:

- The camera must not display any personal elements of your home life, e.g. photographs, calendars etc.
- You must be appropriately dressed as if in the school building
- All Progress Schools policies, procedures and conduct remains the same
- Where staffing ratios allow, a second team member should be in the lesson also

7. Monitoring

7.1 This policy will be monitored through the submission of incident reports relating to offences involving e-safety and technological devices.

7.2 Staff are trained on all aspects of e-safety. Staff are also asked to adhere to the Social Media Guide and refer to other linked policies including the KCSIE (2023) legislation guidance.

7.3 All Progress Schools systems are protected by filtering and monitoring services provided by CNS IT. See Safeguarding and Child Protection Policy for further details.

8. Additional support

8.1 The following websites are extremely helpful when dealing with cyberbullying and e-safety issues.

- **Ceop**
  www.ceop.police.uk
  Child Exploitation and online Protection Centre
- **Bullying Online**
  www.bullying.co.uk
  Advice for children, parents and colleges
- **Virtual College**
  www.safeguardingchildrenea.co.uk
- **Kidsmart**
  www.kidsmart.org.uk
  An Internet safety site from Childnet, with low-cost leaflets for parents.
- **Think U Know?**
  www.thinkuknow.co.uk/
  Home Office site for students and parents explaining Internet dangers and how to stay in control.
- **Safekids**
  www.safekids.com
  Family guide to making Internet safe, fun and productive
- **Maths Doctor**
  http://www.mathsdoctor.co.uk/online/child-safety
  How To Keep Your Child Safe Online
- **UK Safer Internet**

https://www.saferinternet.org.uk/

9. Associated documents

1) Working together to safeguard children (HM Government)
2) Keeping children safe in education (DfE)
3) Revised Prevent Duty (HM Government)

4) Channel Duty Guidance (HM Government)
5) Inspecting safeguarding in early years, education and skills settings (Ofsted)
6) The Education (Independent School Standards) Regulations
7) The Equality Act
8) The Human Rights Act
9) Searching, screening and confiscation in schools
10) Sexting in Schools and Colleges (UK Council for Child Internet Safety)
11) Progress Schools Safeguarding and Child Protection Policy
12) Progress Schools Behaviour and Anti-Bullying Policy