E-SAFETY POLICY

December 2018

Passmores Co-operative Learning Community

Contents:

This policy has been updated in line with the requirements of the General Data Protection Regulation (GDPR), which came into effect on 25 May 2018, to include further information on consent, data security and the responsibilities of the data protection officer (DPO). The updated policy also includes reference to the 2018 version of Keeping Children Safe in Education.

The policy is based on the model by The SchoolBus, released in June 2018

The PCLC Local Governing bodies reviewed the policies in November 2018

The Trustees approved the policy on 17th December 2018. The policy will be reviewed annually, or sooner if updates to legislation are made.

Statement of intent

At Passmores Co-operative Learning Community (PCLC), we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst our schools recognise the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our schools have created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The PCLC is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to mitigate the risk of harm.

Passmores Academy has assigned staff to the following roles:

Designated Safeguarding Lead (DSL) -	Lucy Goddard
E-safety Officer -	Russell King
Data Protection Officer (DPO) -	Tina Sparrow
IT Manager -	Ashley Alderson

1. Legal framework

1.1. This policy has due regard to all relevant legislation including, but not limited to:

- The General Data Protection Regulation
- Freedom of Information Act 2000

1.2. This policy also has regard to the following statutory guidance:

- DfE (2018) 'Keeping children safe in education'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'

1.3. This policy will be used in conjunction with the following school policies and procedures:

- Safeguarding / Child Protection policy
- Anti-bullying policy
- Information Systems and Social Media policy
- Use of Camera and Images policy

2. Use of the internet

2.1. The PCLC understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school is required to implement to minimise harmful risks.

2.3. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including the following:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. content involving radicalisation

- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

3.1. It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.

3.2. The Trust Board is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils. This will be monitored by the PCLC schools own Local Governing Body.

3.3. The e-safety officer, is responsible for ensuring the day-to-day e-safety in the school and managing any issues that may arise.

3.4. The principal/headteacher is responsible for ensuring that the e-safety officer and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.

3.5. The e-safety officer will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach pupils about online safety.

3.6. The principal/headteacher and data protection officer (DPO) will ensure there is a system in place which monitors and supports the e-safety officer, whose role is to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.

3.7. The e-safety officer will regularly monitor the provision of e-safety in the school and will provide feedback to the principal/headteacher.

3.8. The principal/headteacher will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.

3.9. The e-safety officer will ensure that all members of staff are aware of the procedure when reporting e-safety incidents and will keep a log of all incidents recorded.

3.10. The e-safety officer will attempt to find alternatives to monitoring staff use of social media, where possible, and will justify all instances of monitoring to ensure that it is necessary and outweighs the need for privacy. The member of staff who is being monitored will be consulted prior to any interception by the school.

3.11. The Local Governing Body will discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school's duty of care, and will report their findings back to the Trust Board.

3.12. The Local Governing Body will evaluate and review this E-safety Policy on an annual basis, considering the latest developments in ICT and the feedback from staff/pupils.

3.13. The principal/ headteacher will review and amend this policy with the e-safety officer and DPO, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.

3.14. Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.15. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-safety Policy.

3.16. All staff and pupils will ensure they understand and adhere to our Acceptable Use Agreement, which they must sign and return to the principal/headteacher.

3.17. Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

3.18. The principal/headteacher is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

3.19. All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

4. E-safety education

Educating pupils:

4.1. An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.

4.2. Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material, and the validity of website content.

4.3. Pupils will be taught to acknowledge ownership of information they access online, in order to avoid copyright infringement and/or plagiarism.

4.4. Clear guidance on the rules of internet use will be presented in all classrooms.

4.5. Pupils are instructed to report any suspicious use of the internet and digital devices to their classroom teacher.

4.6. PSHE lessons will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.

4.7. The school will hold e-safety events, such as Safer Internet Day and Anti-Bullying Week, to promote online safety.

5.

Educating staff:

5.1. All staff will undergo e-safety training to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole.

5.2. All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.

5.3. All staff will be educated on which sites are deemed appropriate and inappropriate.

5.4. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.

5.5. Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-safety Policy.

5.6. The e-safety officer will act as the first point of contact for staff requiring e-safety advice.

Educating parents:

5.7. E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media.

5.8. Twilight courses and presentations will be run by the school for parents.

5.9. Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any e-safety related concerns.

6. E-safety control measures

Internet access:

6.1. Internet access will be authorised once parents and pupils have returned the signed consent form in line with our Acceptable Use Agreement.

6.2. Where a pupil is over the age of 13 and they fully understand what they are consenting to, parents' consent is not required in line with the GDPR; however, the school will notify parents that the pupil has consented independently.

6.3. A record will be kept by the principal/headteacher of all pupils who have been granted internet access.

6.4. All users in KS2 and above will be provided with usernames and passwords and will be instructed to keep these confidential to avoid any other pupils using their login details.

6.5. Pupils' passwords will expire every 30 days, and their activity is continuously monitored by the e-safety officer.

6.6. Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.

6.7. Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.

6.8. Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.

6.9. The Trustees will ensure that the use of appropriate filters and monitoring systems does not lead to 'over blocking' – unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

6.10. Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the principal/headteacher.

6.11. All school systems will be protected by up-to-date virus software.

6.12. An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.

6.13. Master users' passwords will be available to the principal/headteacher for regular monitoring of activity.

6.14. Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.

6.15. Personal use will only be monitored by the e-safety officer for access to any inappropriate or explicit sites, where the need to do so outweighs the need for privacy.

6.16. Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only and prohibited from using any personal devices. This will be dealt with following the process outlined in the misuse by staff section of this policy.

Email:

6.17. Pupils and staff will be given approved email accounts and are only able to use these accounts.

6.18. The use of personal email accounts to send and receive personal data or information is prohibited.

6.19. No sensitive personal data shall be sent to any other pupils, staff or third parties via email.

6.20. Pupils are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.

6.21. Staff members are aware that their email messages are not monitored.

6.22. Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.

6.23. Chain letters, spam and all other emails from unknown sources will be deleted without opening.

6.24. Staff will not be punished if they are caught out by cyber-attacks as this may prevent similar reports in the future. The e-safety officer will conduct an investigation; however, this will be to identify the cause of the attack, any compromised data and if there are any steps that can be taken in the future to prevent similar attacks happening.

Social networking:

6.25. The use of social media on behalf of the school will be conducted following the processes outlined in our Information Systems and Social Media policy.

6.26. Access to social networking sites will be filtered as appropriate.

6.27. Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the principal/headteacher.

6.28. Pupils are regularly educated on the implications of posting personal data online outside of the school.

6.29. Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole. This includes not posting images of students on any platform where permission to do so has not been expressly granted.

6.30. Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.

6.31. Staff are not permitted to publish comments about the school which may adversely affect its reputation.

6.32. Staff are not permitted to access social media sites during teaching hours unless it is beneficial to the material being taught. This will be discussed with the principal/headteacher prior to accessing the social media site.

7.

Published content on the school website:

7.1. The principal/headteacher will be responsible for the overall content of the website and will ensure the content is appropriate and accurate.

7.2. Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.

7.3. Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully and will not be posted until authorisation from parents has been received.

7.4. Pupils are not permitted to take or publish photos of others without permission from the individual.

7.5. Staff are able to take pictures, though they must do so in accordance with the PCLC Use of Camera and Images policy. Staff will not take pictures using their personal equipment.

7.6. Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

Mobile devices and hand-held computers:

7.7. The principal/headteacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.

7.8. Mobile devices are not permitted to be used during school hours by pupils unless expressly given permission by a member of teaching staff.

7.9. Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the e-safety officer where it is justifiable to do so and the justification outweighs the need for privacy.

7.10. The sending of inappropriate messages or images from mobile devices is prohibited.

7.11. Personal mobile devices will not be used to take images or videos of pupils or staff.

7.12. The DPO will, in collaboration with the e-safety officer, ensure all school-owned devices are password protected.

7.13. To protect, retrieve and erase personal data, all mobile devices and hand-held computers can be fitted with software to ensure they can be remotely accessed.

7.14. ICT technicians and the e-safety officer will review and authorise any apps and/or computer programmes before they are downloaded – no apps or

programmes will be downloaded without express permission from an ICT technician or the e-safety officer.

7.15. Apps will only be downloaded from manufacturer approved stores, e.g. Google Play and the Apple App Store.

Network security:

7.16. Network profiles for each pupil and staff member are created in which the individual must enter a username and personal password when accessing the ICT systems within the school.

7.17. Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.

7.18. Passwords will require a mixture of letters, numbers and symbols to ensure they are secure as possible.

7.19. Passwords will expire after 30 days to ensure maximum security for pupil and staff accounts.

7.20. Passwords should be stored using non-reversible encryption.

7.21. Initial default passwords issued to any user should be changed immediately following notification of account set up using the password criteria below:

- Minimum 7 characters
- Capital letter
- Lower case letter
- Number
- Special character like the asterisk or currency symbol

7.23 The e-safety officer and ICT technicians will ensure all school-owned laptops and computers have their encryption settings turned on or, if there is no built-in encryption option, encryption software is installed.

7.24 Important folders, e.g. those including pupils' medical records, will be password protected to ensure their security – the e-safety officer, school nurse and other designated individual(s) will be the only people who have access to this password.

Virus management:

7.25. Technical security features, such as virus software, are kept up-to-date and managed by the e-safety officer.

7.26. The e-safety officer will ensure that the filtering of websites and downloads is up-to-date and monitored.

7.27. Firewalls will be switched on at all times – ICT technicians will review these on as necessary to ensure they are running correctly and to carry out any required updates.

7.28. Firewalls and other virus management systems, e.g. anti-virus software, will be maintained in accordance with the school's Information Systems Policy.

7.29. Staff members will report all malware and virus attacks to the IT Manager and DPO immediately.

Cyber bullying

7.32. For the purposes of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive messages, or the posting of information or images online. The school recognises that both staff and pupils may experience cyber bullying and is committed to responding appropriately to instances that should occur.

7.33. The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

7.34. Pupils will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.

7.35. The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.

7.36. The school has zero tolerance for cyber bullying, and any incidents will be treated with the utmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy, which includes the policy on cyber bullying.

7.37. The principal/headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

Reporting misuse

7.38. The PCLC schools will clearly define what is classed as inappropriate behaviour in the Information Systems and Social Media Policy, ensuring all pupils and staff members are aware of what behaviour is expected of them.

7.39. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

Misuse by pupils:

7.40. Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.

7.41. Any instances of misuse should be immediately reported to a member of staff, who will then report this to the headteacher using a complaints form.

7.42. Any pupil who does not adhere to the rules outlined in our Acceptable Use Agreement and is found to be wilfully misusing the internet will have a

letter sent to their parents explaining the reason for suspending their internet use.

7.43. Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the principal/headteacher and will be issued once the pupil is on the school premises.

7.44. Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Safeguarding Policy and Child Protection Policy and the PREVENT Duty.

Misuse by staff:

7.45. Any misuse of the internet by a member of staff should be immediately reported to the principal/headteacher, using a complaints form.

7.46. The principal/headteacher will deal with such incidents in accordance with the policy on allegations of abuse against staff (see Safeguarding / Child Protection Policy) and may decide to take disciplinary action against the member of staff.

7.47. The principal/headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

Use of illegal material:

7.48. In the event that illegal material is found on the school's network, or evidence suggests that illegal material has been accessed, the police will be contacted.

7.49. Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.

7.50. 7.50 If a child protection incident is suspected, the school's child protection procedure will be followed – the DSL and principal/headteacher will be informed and the police contacted.

7.51. Staff will not view or forward illegal images of a child. If they are made aware of such an image, they will contact the DSL.

Monitoring and review

7.52. The Trust Board will evaluate and review this E-safety Policy on an annual basis, taking into account the school's e-safety calendar, the latest developments in ICT and feedback from staff/pupils.

7.53. This policy will also be reviewed on an annual basis by the PCLC schools' local governing body and ratified by the Trust Board. Any changes made to this policy will be communicated to all members of staff.

7.54. Members of staff are required to familiarise themselves with this policy as part of their induction programme.

Personal and Sensitive Data Security – Do's and Don'ts for all staff

Passwords – Do

- use a strong password (see Information Systems and Social Media policy for information).

Passwords – Don't

- share your passwords with anyone else or write them down
- save passwords in web browsers if offered to do so.

Devices – Do

- try to prevent people seeing you enter passwords or view sensitive information
- log-off / lock your device when leaving it unattended.

Devices – Don't

- use personal devices to view trust-related or pupil data.

Sending and sharing - Do

- be aware of who you are allowed to share information with. Check with the DPO if you are not sure, who will check that third parties are GDPR-compliant.
- only use encrypted removable media (such as encrypted USB pen drives) if ever taking any personal or sensitive data outside of the trust, which should be **avoided at any cost** and only done with explicit permission from the DPO or IT Manager.

Sending and sharing – Don't

- send sensitive information (even if encrypted) on removable media (USB drives, CDs, portable drives), if secure remote access is available.
- send personal or sensitive information by email unless it is encrypted and use the systems that you are told to use.

Accessing / saving data – Do

- only attempt to access data you are allowed to and save it on locations where the trust knows that data is stored (the trust must know where all data is and be able to access it at all times).

Working on-site – Don't

- leave personal or sensitive information unattended; lock it away in lockable drawers or logoff or lock your work station.
- let strangers or unauthorised people into staff areas or on your PC or device.
- position screens where they can be read from outside the room.

Working off-site – Do

- only take information offsite when you are authorised to and only when it is necessary.
- make sure you sign out completely from any services you have used.
- ensure you save to the appropriate directory to enable regular backups.
- ensure that it is protected offsite in the ways referred to above, access data remotely instead of taking it off-site using approved secure systems.
- only take paper copies off site if it is absolutely necessary and ensure they are not left in a car or public area and are stored safely at home.

General Information and Guidance

What is personal data: any information relating to an identifiable living person, e.g. name,
contact details, ID numbers, attendance and assessment information, financial information

What is sensitive personal data: includes information that reveals someone's ethnic origin,
political opinions, religion, sexuality or health. In our school, it also means safeguarding information, and whether a child is looked-after, has SEN, or is eligible for free school meals

- ✓ Remember that data protection laws DO NOT stop you from reporting safeguarding concerns
  - ➢ You must still report to the relevant people where you're concerned about a child. You do not need anyone's consent to do this
- ✓ Only collect the information you actually need
  - ➢ When you're requesting information (for example, via consent forms, admissions forms or surveys) ask yourself "Do I really need this? What will I actually use it for?"
  - ➢ If you don't need it, or only want it "just in case", don't collect it
  - ➢ If you've already collected personal information that you don't need, delete it
- ✓ Keep personal data anonymous, if possible
  - ➢ For example, if you're emailing a colleague about accommodating a pupil's religion, or about managing a pupil's medical condition, don't name the child if you don't need to
  - ➢ This is particularly important with photographs for external use – if you have an image of a child, don't attach their name to it unless you have explicit consent to do so (student services can give this information or it is available on SIMS on Tab 12 – Parental Consent)
- ✓ Think before you put information up on the wall
  - ➢ If your display is an essential part of teaching and learning, or helps to keep pupils safe, it's fine. This might include medical information, or a list of parents' evening appointments. Still only display the information you really need to
  - ➢ If your display is non-essential, promotional, or there might be a safeguarding risk, either ask the pupil (if aged 13 or over) or check SIMS to ensure we have consent to display it
- ✓ Photograph consent has been sought in the following areas and is available in Tab 12 – Parental Consent on SIMS.
  - ➢ School Website.
  - ➢ School Prospectus
  - ➢ Internal displays (SIMS, Reward Board etc.)
  - ➢ School videos
  - ➢ Press Releases
  - ➢ School Newsletters
  - ➢ School Apps Twitter