Online safety and Acceptable Use Policy

1. Introduction and background

1.1 This policy applies to all members of the Pegasus Academy Trust community (including staff, students, volunteers, parents/carers and visitors) who have access to and are users of the schools' IT systems, both in and out of our settings, for instance when working from home. It should be read in-line with our Safeguarding Policy and 'Keeping Children Safe in Education' (KCSIE) 2025 Annex B and Annex C

1.2 We ask all children, parents, carers and staff within our Trust to adhere to this Online safety and Acceptable Use Policy (AUP) which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media - both when on school site and outside of school. It aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. We aim to help our pupils, their parents/carers and our staff to be responsible users who know how to stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

1.3 The use of technology has become increasingly integral to life in today's society. The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Its use by families, teachers and pupils can benefit all aspects of life, in school and beyond. Current and emerging technologies commonly used by children either in school, outside, or both include:

a) The Internet;
b) E-mail;
c) Instant messaging (e.g. 'Facetime') using camera phones or computer cameras;
d) Video meets through MS teams, GoogleMeet or Zoom;
e) Blogs;
f) Podcasting;
g) Social networking sites;
h) Video broadcasting sites such as 'YouTube';
i) Chat rooms;
j) Gaming sites;
k) Music download sites – Spotify, Itunes;
l) Mobile phones with camera and video functionality and perhaps e-mail and web functionality;
m) Other mobile technology that is 'Internet ready' (e.g. iPads, games consoles, e-readers, smart televisions).
n) AI technologies.

1.4 The potential to enhance teaching and learning through the considered, strategic use of such information technology (IT) is enormous. It can stimulate discussion; promote creativity and increase awareness and understanding to encourage effective learning.

1.5 However, the use of these technologies can put young people at risk. Online safety encompasses not only internet technologies, but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using IT. It provides safeguards and raises awareness to enable users to control their online experiences. Some of the dangers children, and adults, may face when using technology include:

a) Being exposed to unsuitable content, e.g. illegal, harmful or inappropriate images or other content such as video / Internet games;
b) Being subjected to inappropriate, possibly harmful, online interaction with others, including strangers;
c) Loss of/ sharing of/ unauthorised access to personal information, including the sharing or distribution of personal images without the individual's consent or knowledge;
d) Cyber-bullying;
e) Inadvertent / unintentional copyright infringement through plagiarism or illegal downloading of music or video files;
f) An inability to evaluate the quality, accuracy and relevance of information on the Internet, including understanding that AI generated content is not real;
g) The potential for excessive use which can impact on social and emotional development and learning.

1.6 It is difficult to completely eliminate risk and therefore it is essential, through good educational provision, to build pupils' awareness and to give them the confidence and skills to enable them to face and deal with these risks if / when they are exposed to them.

2. Scope of the policy

2.1. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

a) **content:** being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
b) **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
c) **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying;
d) **commerce:** exposure to online shopping traps, fraud, phishing, persuasive marketing, and identity theft

2.2. Creating a safe IT learning environment within the Pegasus Academy Trust includes three main elements:

a) An effective range of technological tools;
b) Policies and procedures, with clear roles and responsibilities;
c) A comprehensive online safety education programme for pupils, staff and parents.

2.3 The Pegasus Academy Trust takes all reasonable precautions to ensure Online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material should never appear on a Pegasus Academy Trust computer or mobile device. The Directors of the Trust cannot accept liability for material accessed or any consequences of Internet access.

2.4 **Purple Mash:** To support the understanding and awareness of constantly evolving online safety issues encountered by children the Pegasus Academy Trust have opted to use the Scheme of Work called '**Purple Mash'** from 2021. As part of its teaching content 'PurpleMash' uses online simulations where, under the guidance of their teacher, pupils can simulate how to use applications safely. For instance, '2Email' is a 'closed system'; to practise emailing skills but emails cannot be sent or received outside the MAT.

3. Roles and Responsibilities

3.1 **Directors of The Pegasus Academy Trust:** Directors are responsible for the approval of the Acceptable Use Policy and have an overview understanding of online safety issues and strategies within the Trust.

3.2 **Members of the Academy Councils** ('MACs' - site specific). We ensure our Academy Council Members are aware of both local and national guidance on online safety. They receive regular monitoring reports about online safety incidents from the Head of Schools.

3.3 **Executive Principals:** Online safety is recognised as an essential aspect of strategic leadership within the Pegasus Academy Trust and the Executive Principals and Heads of School, with the support of Academy Council Members, aim to embed safe practices into the culture of the Pegasus Academy Trust. The Executive Principals are responsible for ensuring the safety (including Online safety) of members of the Pegasus Academy Trust community and ensure that the Online safety Policy is implemented and, along with the Academy Councils, that compliance with the policy is monitored. The Executive Principals, working with the Heads of School, appoint a designated Online safety Coordinator/s to have day to day responsibility for online safety.

3.4 **Heads of School:** The Heads of School are responsible for ensuring that all members of staff, including the Online safety Coordinator, receive suitable training and support to enable them to appropriately carry out their responsibilities with regards to the safe use of IT.

3.5 **The Online safety Coordinator (normally a member/s of the IT team):**

a) Ensure they stay up to date with online safety issues and guidance through liaison with the Local Authority Online safety Officer and through organisations such as The UK Safer Internet Centre and The Child Exploitation and Online Protection (CEOP);
b) Take day to day responsibility for online safety issues;
c) Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
d) Facilitate regular training and advice for staff, including refresher training, on online safety matters;
e) Liaise with IT technical staff as required;
f) Receive reports of online safety incidents and creates a log of incidents to inform future online safety developments;
g) Report regularly to the Senior Leadership Team

3.6 **Network Manager**: The Network Manager is responsible for ensuring:

a) The Pegasus Academy Trust's IT infrastructure is secure and is not open to misuse or malicious attack;
b) Users can only access the Pegasus Academy Trust's networks through a properly enforced password;
c) The Pegasus Academy Trust's filtering policy is appropriately applied and is updated on a regular basis;
d) He/she keeps up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
e) That use of the Pegasus Academy Trust's network, Virtual Learning Environment (VLE), remote access and email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online safety Coordinator;
f) That monitoring software / systems are implemented and updated as agreed in Pegasus Academy Trust policies;

g) Hardware, such as laptops used for home learning are monitored using '*Securely*' to ensure appropriate use in line with the Acceptable Use Policy and practices.

3.7 **Teaching and support staff**: All teaching and support staff are responsible for promoting and supporting safe behaviours. All staff must follow Pegasus Academy Trust online safety procedures in their classrooms and at home when using home learning platforms, such as Google Classroom and Google Meet. Central to this is fostering a 'No blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials. Teachers and support staff should also ensure that:

a) They have read, understood and signed the Pegasus Academy Trust Staff Acceptable Use Agreement;
b) They have an up to date awareness of online safety matters and of the current Pegasus Academy Trust Acceptable Use Policy and practices, including:

i. Safe use of e-mail;
ii. Safe use of Internet including use of Internet-based communication services such as instant messaging and social network;
iii. Safe use of the Pegasus Academy Trust network, equipment and data;
iv. Safe use of digital images and digital technologies, such as mobile phones, digital cameras and hand held devices;
v. Appropriate publication of pupil information/photographs and use of website;
vi. Cyber-bullying procedures.

c) They understand their role in providing online safety education for pupils to ensure that online safety issues are embedded in all aspects of the curriculum and other activities so that pupils understand and follow the Pegasus Academy Trust Acceptable Use Policy and know how to minimise online risks and report problems;
d) Pupils have an understanding of how to conduct research on the Internet;
e) ICT activity in lessons / extra-curricular and extended school activities is appropriately supported and monitored;
f) Whenever Internet use is pre-planned, pupils are guided to sites which have been checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches;
g) Pupils understand how to use home learning platforms effectively and appropriately;
h) Any digital communications with pupils or parents / carers (via email / Virtual Learning Environment (VLE) / voice) are on a professional level and carried out using official Pegasus Academy Trust systems;
i) Any suspected ICT misuse or online safety problem is reported to the Online safety Coordinator (and Designated Safeguarding Lead, if applicable) for investigation / action / sanction

3.8 **Designated safeguarding leads (DSLs):** All designated safeguarding Leads are trained in online safety issues as stated in KCSiE 2025 and are aware of the potential for serious child protection issues arising from the sharing of personal data, access to inappropriate materials, inappropriate on-line contacts or cyber-bullying.

3.8.1 We understand that many children have unlimited and unrestricted access to the internet out of school hours via mobile phone networks. This access means that some of our children have the potential to harass their peers via their mobile and smart technology, share indecent images, consensually and non-consensually (often via large chat groups), and view and share other harmful content. We work with parents to make them aware of the risk of unmonitored internet use via newsletters, parent events and meetings with affected families. DSLs are involved in this process as required by the Head of School at a particular site.

3.8.2 Within The Pegasus Academy Trust we manage this risk and protect children from inappropriate content, without unreasonably impacting teaching and learning, through our filtering and monitoring systems. We also aim to keep children safe when they are accessing online learning and are not in school. Annex B of KCSIE provides additional information and support for schools and parents to keep children safe online.

3.8.3 "Securely" is the filtering and monitoring product we use on Chromebooks. It has the benefit of alerting DSLs if for example children access the Childline website, or search about self harm. The Trust's filtering and monitoring systems are provided through London Grid for Learning and are reviewed at least annually.

3.9 Pupils:

a) Are responsible for using the Pegasus Academy Trust IT systems in accordance with the Pupil Acceptable Use Agreement, which they (or their parent / carer) should be expected to sign when they join the school;
b) Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
c) Are expected to know and understand Pegasus Academy Trust policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand Pegasus Academy Trust policies on the taking / use of images and on cyber-bullying;
d) Should understand how to safely use the Internet to research a subject;
e) Should understand the importance of adopting good online safety practice when using digital technologies and home learning platforms out of school and realise that the Pegasus Academy Trust's Online safety Policy covers their actions out of school, if related to their membership of the Pegasus Academy Trust.

3.10 Parents and carers: Parents and carers play an essential role in the education of their children. In partnership with the Pegasus Academy Trust they are responsible for:

a) Ensuring their children understand the need to use the Internet and mobile devices in an appropriate way;
b) Monitoring / regulating their children's on-line use and experiences at home;
c) Endorsing (by signature) the Pupil Acceptable Use Agreement (see Appendix);
d) Ensuring they and their children access the Pegasus Academy Trust website and VLE in accordance with the Acceptable Use Agreement;
e) Reinforcing the need for their child to adopt good online safety practice when using digital technologies and home learning platforms out of school where this relates to their membership of the Pegasus Academy Trust;

4. Technical Infrastructure

4.1 The Pegasus Academy Trust, through its appointed IT support service provider, is responsible for ensuring that the Trust's and its schools' infrastructure and networks are as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It should also ensure that the relevant people are effective in carrying out their online safety responsibilities.

4.2 General technical safety:

a) Pegasus Academy Trust IT systems should be managed in ways that ensure that the Trust, and its individual schools, meet all online safety technical legislation;
b) Servers, wireless systems and cabling should be securely located and physical access restricted;

c) All users should have clearly defined access rights to Pegasus Academy Trust ICT systems. Details of the access rights available to groups of users should be recorded by the Network Manager and should be regularly reviewed.

4.3 Usernames and passwords:

a) All staff should be issued with usernames and passwords to enable them to access Pegasus Academy Trust computers, networks and systems. Users are required to change their password every 90 days in accordance with LGfL policy;
b) All pupils in KS1 and 2 should be provided with a username and password;
c) An up to date record of staff users, usernames and passwords should be accessible only to registered, trained system administrators including the Heads of School. Pupil logins are available for all teaching staff.
d) The "master / administrator" passwords for the Pegasus Academy Trust ICT systems should be available to the Executive Headteachers or other nominated senior leaders and should be securely kept. Staff at this level of access will generally have a 'One time password' (OTP) for their interactions with the LGfL;
e) All users should be made aware of the need to be responsible for the security of their username and password and that they must immediately report any suspicion or evidence that there has been a breach of security.

4.4 Filtering and security: Despite careful design, filtering systems cannot be completely effective due to the speed of change of Web content. At the Pegasus Academy Trust:

a) We use the managed filtering service provided by the LGfL; The following links explain our filtering and monitoring systems in depth:

   i. https://d1xsi6mgo67kia.cloudfront.net/uploads/2020/01/LGfL-Appropriate-Filtering-Provider-Response-August-2023-LGfL.pdf
   ii. https://cyberdistribution.co.uk/student-safety/

b) We work in partnership with parents, the LA, DfE and LGfL to ensure systems to protect pupils are reviewed and improved;
c) If staff or pupils discover unsuitable sites, the URL (address) and content should be reported immediately to LGfL via raising a support ticket. Technical staff will then bring this to the attention of the Online safety co-ordinator;
d) Senior staff should ensure that ongoing checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;
e) ICT technical staff will regularly monitor and record the activity of users on the Pegasus Academy Trust IT systems and users should be made aware of this through the Acceptable Use Agreement;
f) Appropriate security measures, including up to date virus software, should be in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices, etc. from accidental or malicious attempts which might threaten the security of the Pegasus Academy Trust systems and data;
g) All staff and pupils (or their parent / carer on their behalf) should read and sign the 'Acceptable IT Use Agreement' before using any IT resource;
h) Personal data should not be sent over the Internet or taken off the school site unless safely encrypted or otherwise secured;
i) An agreed policy should be in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the Pegasus Academy Trust system;
j) An agreed policy should be in place regarding the downloading and / or installation of executable files and programmes on Pegasus Academy Trust workstations / portable devices by users;

k) An agreed policy should be in place regarding the extent of personal use that users and their family members are allowed to use laptops and other portable devices out of school;
l) An agreed policy should be in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) on Pegasus Academy Trust devices. As the Trust provides remote access options the use of these devices should be limited to circumstances when these systems aren't working;
m) An agreed policy should be in place regarding the use, by staff members, of personal technology and devices for work purposes (e.g. mobile phone, digital camera, personal computer, hand-held device).
n) An agreed policy is in place regarding the use, by pupils and staff, of school hardware such as laptops, Ipads and chrome books for home learning purposes. These documents were created for COVID-19 loans in 2020 and are available from SLT

4.5 Internet access (curriculum)

a) The Pegasus Academy Trust should allocate internet access for staff and pupils on the basis of educational need. Parental permission should be gained, through the home-school agreement, before access is permitted.

4.6 E-mail and communications: The government encourages the use of email as an essential means of communication. Educationally, directed email use can bring significant benefits and support interesting projects between schools. However, the use of email requires that appropriate safety measures are put in place. Unregulated email can provide a means of access to pupils, which bypasses the traditional school boundaries. Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content and viruses can be used to control and monitor material. When using communication technologies Pegasus Academy Trust considers the following as good practice:

a) The official Pegasus Academy Trust email service may be regarded as safe and secure and is monitored;
b) Staff should preferably **only use** the Pegasus Academy Trust email service to communicate with others about school matters;
c) Staff should use 'Egress' when sharing confidential or sensitive information with outside agencies such as social care and health care professionals**.**
d) Any digital communication between staff and parents / carers (email, chat, VLE etc.) is discouraged. If it is deemed necessary, usually with the agreement of a member of the SLT, it should be professional in tone and content. These communications should only take place on official (monitored) Pegasus Academy Trust systems, preferably via the main school office e-mail accounts or blogs. Personal email addresses, text messaging or public chat / social networking programmes should not be used for these communications;
e) Currently e-mail is not used by children in Key Stage 1. Pupils at KS2 are provided with individual school email addresses for educational use and should only use these accounts on the school system;
f) Pupils should immediately tell an adult (and staff should immediately report this to the nominated person, in accordance with the Pegasus Academy Trust policy) of the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and should not respond to any such email;
g) Pupils should not reveal personal details of themselves or others, such as addresses or telephone numbers, or arrange to meet anyone in email communication;
h) Pupils' email addresses do not give the full name of the child, and they contain numbers which are irrelevant to an outsider;
i) In some cases a 'group' email address may be used;
j) Access in school to external personal email accounts should be discouraged - e.g. Hotmail accounts;

k) Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material. The forwarding of chain letters is banned;
l) All email (both incoming and outgoing) is checked for banned words and for viruses. Any breach of content is reported and dealt with.
m) Pupils and staff should be aware that school email communications may be monitored.

4.7 **Data protection.** Personal data should be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

a) Fairly and lawfully processed;
b) Processed for limited purposes;
c) Adequate, relevant and not excessive;
d) Accurate;
e) Kept no longer than is necessary;
f) Processed in accordance with the data subject's rights;
g) Secure;
h) Only transferred to others with adequate protection

4.7.1 Staff should ensure that at all times they:

a) Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
b) Use personal data only on secure, password-protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data;
c) Transfer data using encryption and secure password-protected devices.

4.7.2 Personal data should not normally be stored anywhere other than on the Pegasus Academy Trust servers. As the Trust has excellent remote access facilities USB sticks should not be needed and should not be used.

4.8 **Digital images**. The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the Internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the Internet. Those images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out Internet searches for information about potential and existing employees. The Pegasus Academy Trust should inform and educate users about these risks and should implement policies to reduce the likelihood of the potential for harm:

a) When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images, including highlighting the risks attached to publishing personal images on the Internet e.g. on social networking sites;
b) Staff are allowed to take digital/video images to support educational aims, but should follow Pegasus Academy Trust policies concerning the sharing, distribution and publication of those images;
c) Digital images should normally only be taken on Pegasus Academy Trust equipment. Personal equipment should not routinely be used for such purposes;
d) If the use of personal equipment cannot be avoided, images/videos should be downloaded (preferably before the end of the day) to an appropriate place on the Pegasus Academy Trust servers and deleted from the personal equipment.

e) Care should always be taken when taking digital/video images that pupils are appropriately clothed;
f) Pupils should not take, use, share, publish or distribute images of others without their permission.

4.9 The Pegasus Academy Trust website: The security of staff and pupils is essential. Strategies include using relatively small photographs of groups of pupils and using photographs that do not show faces clearly, if at all. At the Pegasus Academy Trust:

a) We require written permission from parents or carers should be obtained (via the Home – School agreement) before photographs of pupils are published on the Pegasus Academy Trust website;
b) Photographs published on the Pegasus Academy Trust website, or elsewhere that include pupils should be selected carefully and should comply with good practice guidance on the use of such images;
c) Pupils' full names should not be used anywhere on a Pegasus Academy Trust website or blog, particularly in association with photographs. The publishing of names with photographs is not acceptable where the names of individual children can be deduced; web images could be misused and individual pupils identified.
d) The point of contact on the web site should be the Pegasus Academy Trust / school address, email and telephone number. Staff or pupils' home information should not be published only official email addresses should be used to identify members of staff.
e) The Executive Headteacher/s take overall editorial responsibility and ensure that content is accurate and appropriate.

4.10 Google Meets: Google meets allow staff and children to meet virtually when remote learning is implemented. At the Pegasus Academy Trust:

a) At least two adults (e.g. teacher/TA) are normally present in the Meet;
b) The adult responsible for meeting administration has the rights to mute pupils individually and remove pupils from the session;
c) The Pegasus Academy Trust expect pupils and parents to present and conduct themselves appropriately at all times during Google Meet sessions;
d) The Trust operates a 'one warning before exit' policy for inappropriate comments in Google Meet chat. Parents will be called to discuss why it was necessary to exit a pupil;
e) Expectations for the session are displayed on screen at the beginning of the meeting;
f) All participants must be informed at the beginning of a session that the session will be recorded and be given the opportunity to leave;
g) Recordings are saved in staff Google Drives and are kept for 2 weeks before being automatically deleted.

4.11 Social networking, chat rooms and personal publishing:

a) The Pegasus Academy Trust blocks/filters access to social networking sites and chat rooms, but may allow them for specific, supervised activities;
b) Newsgroups should be blocked unless a specific use is approved;
c) Children should be advised never to give out personal details of any kind which may identify them or their location.

4.12 Emerging technologies:

a) Emerging technologies should be examined for educational benefit and a risk assessment should be carried out before use within the Pegasus Academy Trust is allowed.

4.13 **Home learning device loans:** When required the Pegasus Academy Trust is able to loan identified pupils laptops, ipads and chrome books to ensure they are able to access learning from home. This IT is managed remotely using 'Neverware' and ''Securly this allows the Trust to turn the equipment off if not used according to the device loan agreement.

a) Parents and pupils must sign the Pegasus Academy Trust device loan agreement before any hardware is released to them. This agreement covers the period from the date the device is issued through to the return date of the device to the school;
b) The device must be returned in its original condition to the Trust within 7 days of recall;
c) All issued equipment shall remain the sole property of the Pegasus Academy Trust and is governed by the Trust's policies;
d) Pupils are responsible for the equipment at all times whether on the school's property or not;
e) The pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person;
f) If equipment is damaged, lost or stolen, parents must immediately inform the school through the admin e-mails on the Trust's website. If the equipment is stolen, parents must immediately inform the police;
g) Equipment must only be used between 0800 and 2130 after which parents must ensure that the equipment is turned off;
h) To ensure appropriate use the school monitors pupil activity on devices and can remotely disable the equipment at any time;
i) Pupils must not carry out any activity that constitutes 'unacceptable use' as described in the Device Loan Agreement;
j) The Trust may sanction the pupils in line with the behaviour policy if pupils engage in 'unacceptable use'.

5. Inappropriate use

5.1 The Pegasus Academy Trust believes that certain activities would be inappropriate in a school context and that users should not engage in these activities in school or outside when using Pegasus Academy Trust equipment or systems. The Pegasus Academy Trust policy restricts certain Internet usage per Table 1 below:

Table 1

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images					X
	Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					X
	Adult material that potentially breaches the Obscene Publications Act in the UK					X
	Criminally racist material in UK					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Promotion of racial or religious hatred				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the Pegasus Academy Trust or brings the Trust into				X	
Using Pegasus Academy Trust systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by LGfL and / or the Pegasus Academy Trust					X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the Internet					X	
On-line gambling					X	
On-line gaming (non educational) – choices are limited by 'Neverware'			X			
On-line gaming (educational)			X			
On-line shopping / commerce			X			
File sharing			X			
Use of social networking sites			X			
Use of video broadcasting e.g. YouTube			X			

5.2 Responding to misuse / complaints. It is hoped that all members of the Pegasus Academy Trust community will be responsible users of IT, who understand and follow this policy.

However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. It is most likely that incidents which arise will involve inappropriate rather than illegal misuse. It is important that any inappropriate use incidents are dealt with as soon as possible, in a proportionate manner and that members of the Pegasus Academy Trust community are aware that they have been dealt with. It is intended that incidents of inappropriate use should be dealt with through normal behaviour / disciplinary procedures.

5.3 If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see below) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Misuse or complaints will be responded to in the following manner:

a) Our Online safety Coordinator/s act as first point of contact for any complaint;
b) Complaints about staff misuse should be referred to the Head of School or Executive Headteacher;
c) Complaints related to child protection are dealt with in accordance with Pegasus Academy Trust / LA child protection procedures;
d) Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy;
e) Children and parents should be informed of the complaints procedure;
f) Discussions should be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

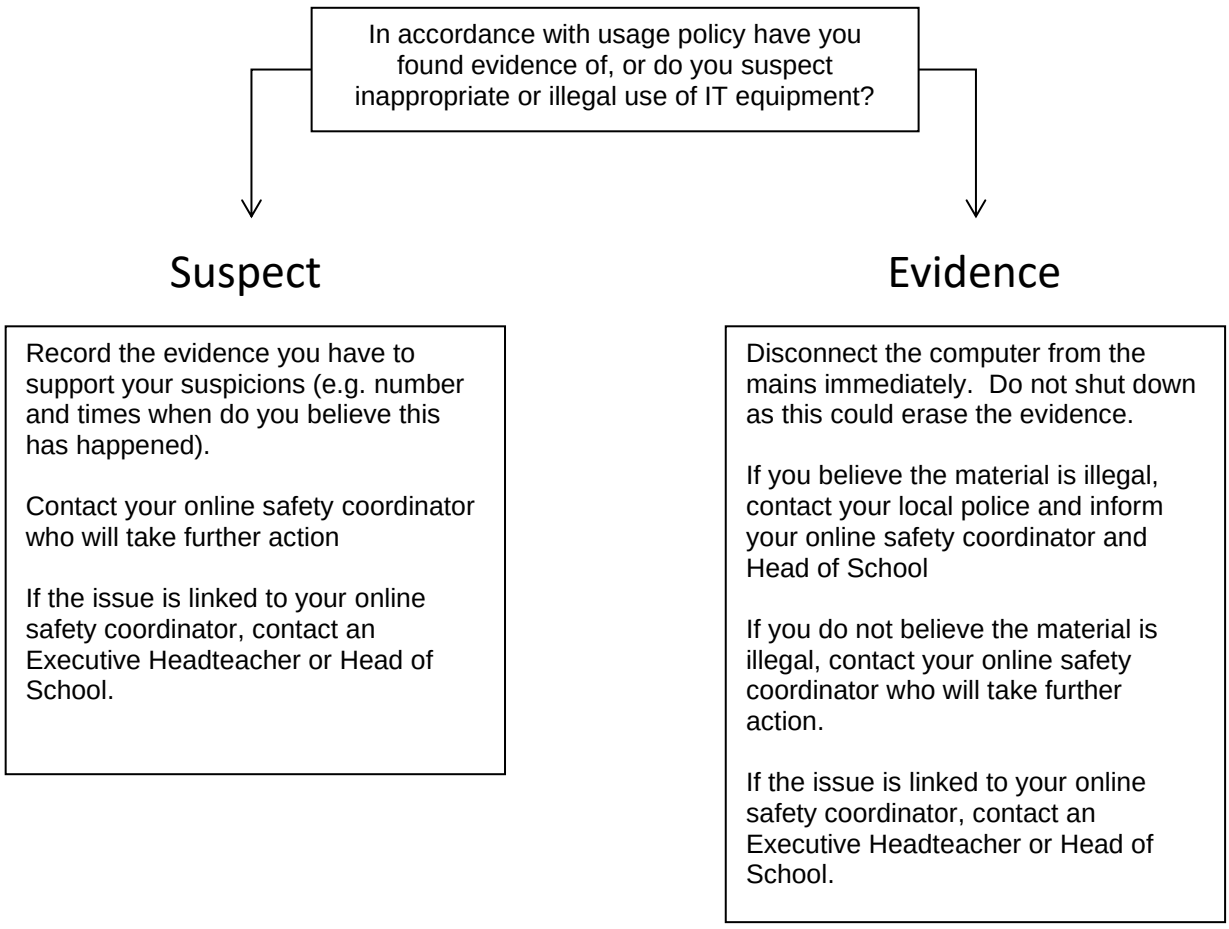
5.4 Staff and pupils should be given information about infringements in use and possible sanctions. Sanctions available include:

a) Discussion with Class Teacher / Head of Year / Online safety Coordinator / Head of School;
b) Informing parents or carers;
c) Removal of Internet or computer access for a period;
d) Referral to LA / Police.

5.5 If any apparent or actual misuse appears to involve illegal activity or material the flow chart below should be consulted and actions followed, in particular the sections on reporting the incident to the police and the preservation of evidence.

Illegal activity involves:

a) Child sexual abuse images;
b) Adult material which potentially breaches the Obscene Publications Act;
c) Criminally racist material;
d) Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation;
e) Other criminal conduct, activity or materials.



6. Monitoring and review

6.1 This policy is regularly reviewed by SLT and a summary of changes made in the revision history – section 7 below.

7. Revision history

Date	Summary of changes
September 2022	• 4.7 expressly discouraging use of USB keys updated; • Section referencing class blogs removed; • Reformatting and typos addressed; • KCSIE references at 1.1 updated and referenced; • 'ICT' changed to 'IT' throughout
September 2023	• Updates from KCSIE 2023 included at 3.8.1-3.8.3 and at 4.4
V5 December 2025	• Added 'commerce' section at [2.1] in line with latest KCSiE guidance; • 'E-safety' replaced with 'Online safety'; • References to emerging AI risk added