Cambridge Park Academy
On-line Safety Policy

Created By:	**D Gardiner**
Approved by;	**Full Governing Body**
Version:	**4**
Created on:	**January 2023** **Updated September 2025**
Next Review Date;	**September 2026**

Policy Statement

For clarity, the On-line Safety policy uses the following terms unless otherwise stated:

- Users - refers to all staff, pupils, governors, volunteers and any other person working in or on behalf of the school, including contractors.
- Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.
- School – any school business or activity conducted on or off the site, e.g. visits, conferences, trips etc.

Safeguarding is a serious matter; at Cambridge Park Academy we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e- safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an On-line Safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Cambridge Park website; upon review all members of staff will sign as read and understood both the Online Safety Policy and the Staff IT Acceptable Usage Policy. A copy of this policy and the Students IT Acceptable Usage Policy will be sent home with students at the beginning of each academic year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, pupil will be permitted access to school's technology including the Internet.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any Online Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure Online Safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of Online Safety at the school who will:

- Keep up to date with emerging risks and threats through technology use

- Receive regular updates from the Principal in regards to training, identified risks and any incidents.

Principal (S Kernan)

Reporting to the governing body, the Principal has overall responsibility for Online Safety within our school. The day-to-day management of this will be delegated to a member of staff, the Online Safety Officer (or more than one), as indicated below.

The Principal will ensure that:

- On-line Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents.
- The designated Online Safety Officer(s) has had appropriate training in order to undertake the day to day duties.
- All Online Safety incidents are dealt with promptly and appropriately.
- Training and Policy is in line with the Online Safety Act 2025

Designated safeguarding lead / On-line Safety (D. Gardiner) Deputy Safeguarding Lead (DSL)

The Designated Safeguarding Lead (DSL) should take the lead responsibility for safeguarding and child protection, including On-line Safety, as per Keeping Children Safe in Education. However, the DSL may delegate certain On-line Safety functions to other members of the school e.g. ICT Support Services.

The day-to-day duty of Online Safety Officer is devolved to D. Gardiner.

The DSL On-line Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Principal.
- Advise the Principal, governing body on all Online Safety matters.
- Engage with parents and the school community on On-line Safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the Online Safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical Online Safety measures in the school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make themselves aware of any reporting function with technical Online Safety measures, i.e. internet filtering reporting function; liaise with the Principal and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored, and devices updated as appropriate.

    - Any Online Safety technical solutions such as Internet filtering are operating correctly.
- Passwords are applied correctly to all user accounts adhering to complexity settings. Age-appropriate passwords are set for pupils by the class teacher, or administrator.
- Passwords for staff will be a minimum of 8 characters.
- Staff passwords will expire every 60 days, and a new unique password must be selected.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood, it should be brought to the attention of the Principal.
- Any Online Safety incident is reported to the Online Safety Officer (and an Online Safety Incident report is made), or in their absence to the Principal. If you are unsure the matter is to be raised with the Online Safety Officer or the Principal to make a decision.
- All online material is checked fully before using either within the classroom or remotely
- The DSL is informed if this policy does not reflect practice, or if concerns are not acted upon promptly.

All pupils

- The boundaries of use of ICT equipment and services in this school are given in the pupil IT Acceptable Usage Policy (Annex A); any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.
- Online Safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly, all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

- Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge, they need to ensure the safety of children outside the school environment. Through parent's evenings, school newsletters, website, the school will keep parents up to date with new and emerging Online Safety risks, and will involve parents in strategies to ensure that pupils are empowered.
- If a trend of Online Safety breaches is found, both staff training and pupil's guidance (assemblies or lessons) will be delivered to educate on this particular trend.
- Parents must also understand the school's needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student IT Acceptable Usage Policy before any access can be granted to school ICT equipment or services.

Technology

- Cambridge Park Academy uses a range of devices including PCs, Laptops, iPads and Chromebooks. In order to safeguard the pupils and in order to prevent loss of personal data we employ the following assistive technology:
- Internet Filtering – we use a Smoothwall Filter managed by our Internet Service Provider that prevents unauthorized access to inappropriate online content. Appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy, or in response to an incident, whichever is sooner. The ICT Coordinator, Online Safety Officer and IT Support

are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Principal and IT support. If staff or pupils discover unsuitable sites, the URL and content must be reported to the On-line Safety lead and IT Support and appropriate measures will be taken to ensure safety.

- The DSL and IT manager meet on a weekly basis to review any concerns or alerts from the previous week. Alerts that are deemed serious are acted upon immediately. All members of SLT and the Safeguarding team are alerted to alerts linked to forms of abuse.
- Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) must be encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device) is to be brought to the attention of the Principal immediately. The Principal will liaise
  with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.
- Passwords – All staff and pupils will be unable to access any device without a unique username and password, except for classroom iPad's that are used under staff supervision. Staff and pupil passwords will change on a regular basis or if there has been a compromise, whichever is sooner. IT Support will be responsible for ensuring that passwords are changed.
- Anti-Virus – All capable devices will have anti-virus software. IT Support will be responsible for ensuring this task is carried out, and will report to the Principal if there are any concerns. IT Support will continue to monitor and update anti-virus software.

Safe Use

- Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this Online Safety and the staff Acceptable Use Policy; pupils upon signing and returning their acceptance of the Acceptable Use Policy.
- Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly, use of personal email addresses for work purposes is not permitted.
- Photos and videos – Working with children and young people may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well-being of children and young people. Informed written consent from parents or carers and agreement, where possible, from the child or young person, should always be sought before an image is taken for any purpose.
- Social Media – there are many social media services available including facebook; Cambridge Park Academy is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within the school and have been appropriately risk assessed; should staff wish to use other social media; permission must first be sought via the DSL who will advise the Principal for a decision to be made. Any new service will be risk assessed before use is permitted.
- Facebook used by the school as an information broadcast service (see below).
- Pupils to use a numbered equipment so that it is traceable.
- Pupils to be monitored by a member of staff whilst using ICT equipment.

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

- In addition, the following is to be strictly adhered to:
    - Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
    - There is to be no identification of pupil using first name and surname; first name only is to be used.
    - Where services are "comment enabled", comments are to be set to "moderated".
    - All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e., creative commons).

- Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day after notification.

Incidents

It is vital that all staff recognise that Online Safety is a part of safeguarding. The Trust 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 on pupils when they come into 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 suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson. Any concern/allegation about staff misuse is always referred directly to the Principal, unless the concern is about the Principal in which case the compliant is referred to the Chair of the Trust and the LADO (Local Authority's Designated Officer). The school will actively seek support from other agencies as needed (i.e. the local authority - Children's Social Care, National Crime Agency, CEOP, Police, IWF). We will inform parents/carers of On-line 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.

Any Online Safety incident is to be brought to the immediate attention of the DSL, or in their absence the Principal. The DSL will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum

It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Cambridge Park Academy will have an annual programme of training which is suitable to the audience.

On-line Safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupil's learning. On-line Safety messages are constantly revisited e.g. participating in national On-line Safety week, ICT & PSHE curriculum etc.

As well as the programme of training, we will establish further training or lessons as necessary in response to any incidents.
All staff to receive training on Artificial Intelligence use and risks.

Annex A

Pupil ICT use agreement

Dear Parents/Carers

Keeping Safe Online we are increasingly conscious that all children and young adults are using technology as part of day to day life – whether this is for work or entertainment, we need to take every measure in order to keep them safe online.

As part of the latest Keeping Children Safe in Education (KCSIE) guidance, and in line with our own online safety expectations, we are trying to really focus on the steps that we can take to keep our pupils safe online both in school and outside of school.

As part of this programme, we have drawn up a Keeping Safe Online Charter which we hope will support our pupils to remain safe and vigilant when using technology.

Please can we ask that you read and discuss this agreement with your child (where this is possible) and then sign it and also ask your child to sign it where they are able to. We will be referring to this charter every time we use computing equipment within the school day. If we could then ask you to return it to the Class Teacher who will be able to support, you further if needed!

Please see the Charter overleaf!

Many thanks for your continued support,

Mrs S French (Assistant Principal)

Agreement:

- I will be support to/I will aim to make safe and smart choices when I am on the internet, whether playing games, using apps, or on social media.
- I will be supported to/aim to make sure that the words I use do not intentionally hurt others.
- I will be supported to/I will aim to use the internet in a responsible way.
- I will be supported to/aim to not send anything that might scare, hurt, or make someone sad.
- I will keep my information safe, including my name, phone number, or where I live on the internet. It's information just for me and the people I trust.
- I won't share my secret passwords with anyone. They are just for me to keep safe.
- I will allow an adult to keep me safe my checking my devices and online activities.
- If something on the internet bothers me or I get a message that makes me sad, I can always talk to _____.

Parent/ Carer Name: _____
Signed: _____
Student name: _____
Signed: _____
Date: _____

Annex B

ICT Acceptable Use Policy (HET) for Staff please see under separate policy.