Internet Acceptable Use Policy

Statement

As part of Chaigeley School's wider duty of care it will ensure that children and young people are able to use the internet and related communications technologies safely and appropriately. It will do this by creating an infrastructure of whole school awareness, designated responsibilities, policies and procedures. The Principal, with the support of the governors, will take a lead in embedding safe internet practices into the culture of the school

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and children.

The aim of this Internet Acceptable Use Policy Statement (IAUPS) is to ensure that children will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. Therefore, if the school IAUPS is not adhered to this privilege will be withdrawn and appropriate sanctions outlined in the IAUPS will be imposed.

School's Strategy

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

General

- Internet sessions should always be supervised by a teacher/carer.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- Access to areas of the Internet is determined by active directory profile type.
- The school will regularly monitor children's Internet usage.
- Children and teachers/carers will be provided with training in the area of Internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of personal memory sticks, CD-ROMs, or other digital storage media in school
- Children should treat others with respect at all times and will not undertake any actions that may bring the school into disrepute

World Wide Web

- Children should not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.

- Children should report accidental accessing of inappropriate materials in accordance with school procedures.
- Children should use the Internet for educational purposes or for recreational purposes in designated timetable slots.
- Children should not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
- Children should never disclose or publicise personal information.
- Downloading materials or images not relevant to their studies, is in direct breach of the school's Acceptable Use Policy.
- Children should be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.
- Wireless access keys will be input by staff on approved devices only and not given to children.

Email & Social Media Safety

- Children should use approved class email accounts under supervision by or permission from a teacher.
- Children should not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
- Children should not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Children should never arrange a face-to-face meeting with someone they only know through emails or the internet.
- Children should note that sending and receiving email attachments is subject to permission from their teacher.
- Children should only have access to chat rooms, discussion forums, messaging or other electronic communication forums that have been approved by the school.
- Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.
- Usernames should be used to avoid disclosure of identity.

School Website and Virtual Learning Environment (VLE)

- Children should be given the opportunity to publish projects, artwork or school work on the World Wide Web in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website. Such material will only be published after verification by the school ICT Co-ordinator
- The website should be regularly checked to ensure that there is no content that compromises the safety of children or staff.
- Website using facilities such as guestbooks, noticeboards or weblogs should be checked frequently to ensure that they do not contain personal details.
- The publication of children's work should be co-ordinated by a teacher.
- Childrens work should appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.

- The school should endeavour to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual children will not be published on the school website without parent/carer permission. Video clips may be password protected.
- Personal child information including home address and contact details should be omitted from school web pages.
- The school website should avoid publishing the full names of children in a photograph.
- The school should ensure that the image files are appropriately named – should not use children's names in image file names or ALT tags if published on the web.
- Children should continue to own the copyright on any work published.
- Children, teachers and carers will have access to the school VLE by approved logon.

Personal Devices

Children are prohibited from using their own mobile phones in school. In some circumstances and under the consideration of the Senior Leadership Team individual personal items, such as mobile phones, used in breach of this policy may be confiscated. Confiscated items will always be returned to parents and carers of children and not to the children themselves, unless the use of the item was in order to aid inappropriate or criminal activity in which the police have to be involved. In such cases the item will always be handed over to the police to aid any necessary investigations.

Legislation

The school will make available, if requested, information on the following legislation relating to use of the Internet which teachers, children and parents/carers can familiarise themselves with:

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988
- Computer Misuse Act 1990
- GDPR (From May 25th 2018)

Support Structures

The school will inform children and parents/carers of key support structures and organisations that deal with illegal material or harmful use of the Internet.

Sanctions

The school reserves the right to:

a) Deny all further access to relevant computer, computer system or computer networks for a defined and limited period.
b) Recover all reasonable costs howsoever incurred in investigating and subsequent restitution of computer, computer systems and computer networks resulting from any misuse or violation of policy.

c) Confiscate any personal items that are used in breach of this policy. Items will always be returned as detailed above.
d) Refer any possible criminal action to the police.

Committee	Date Amended	Review Date
Source: Curriculum	Date: 02.2018	Review: 02:2020