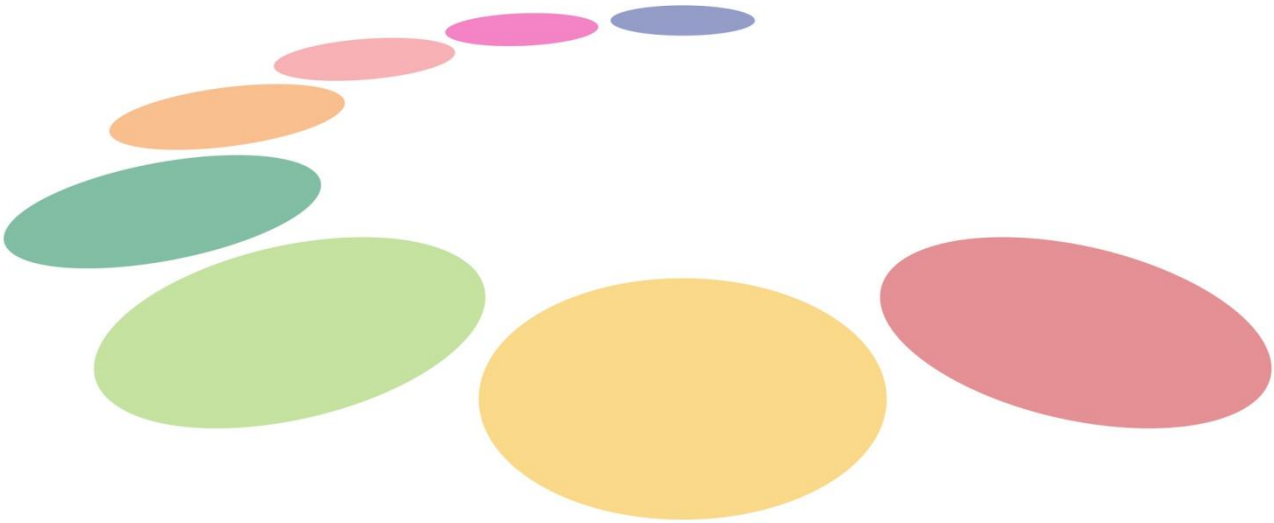
Claremont Primary School

E-Learning Policy



Agreed Date	**Mar 18**
Review Date	**Mar 20**

***Non-Statutory Policy to be reviewed bi-annually by the Headteacher**

Contents

Framework

This policy has due regard to the following legislation, including, but not limited to:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997

This policy also has regard to the following statutory guidance:

- DfE (2016) 'Keeping children safe in education'

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

- Anti- Bullying Policy
- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement
- Behaviour and Discipline Policy
- Safeguarding Policy

1 Introduction

1.1 This policy has been developed to ensure that all adults in Claremont Primary School are working together to safeguard and promote the welfare of children and young people.

1.2 E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

1.3 This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities by using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

1.4 The Headteacher or, in their absence, the Deputy Headteacher is the authorised member of staff for e-safety has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

1.5 This policy complements and supports other relevant school and Local Authority policies.

1.6 The purpose of internet use in school is to help raise educational standards, promote pupil achievement, and support the professional work of staff as well as enhance the school's management information and business administration systems.

1.7 A risk assessment will be carried out before children and young people are allowed to use new technology in schools and settings.

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

- 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

2 Ethos

2.1 It is the duty of the school to ensure that every child and young person in its care is safe. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

2.2 Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures.

2.3 All staff have a responsibility to support e-safe practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols.

2.4 E-safety is a partnership concern and is not limited to school premises.

2.5 Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will dealt with in accordance with the school's Anti-Bullying and Behaviour and Discipline Policy.

2.6 Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy.

3 Roles and Responsibilities

3.1 The Headteacher will ensure that:

- All staff should be included in E-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- A Designated Senior Member of Staff is identified and receives appropriate on-going training, support and supervision and works closely with the Designated Person for Safeguarding.
- All temporary staff and volunteers are made aware of the school's Acceptable Use Policy and arrangements.
- a commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.
- any reports regarding to inappropriate access to websites (key words) using the school filtering system will be monitored. Action will be taken if deemed necessary.

- amend and review the policy taking into account new legislation, government guidance and previously reported incidents to improve procedures
- all staff and volunteers understand and aware of the school's E-Learning/Safety Policy.
- the school's ICT systems are regularly reviewed with regard to security.
- the virus protection is regularly reviewed and updated.
- There are regularly check files on the school's network.

3.2. The Governing Body of the school will ensure that:
- there is a senior member of the school's leadership team who is designated to take the lead on E-Learning/Safety within the school.
- procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority procedures.
- all staff and volunteers have access to appropriate ICT training.
- there are appropriate filtering and monitoring systems in place to safeguard pupils
- the e-learning policy will be reviewed, taking into account the latest IT developments

4 Teaching and Learning

Benefits of internet use for education

4.1 The internet is a part of the statutory curriculum and a necessary tool for staff and children and young people and benefits education by allowing access to world – wide educational resources including art galleries and museums as well as enabling access to specialists in many fields for pupils and staff.

4.2 Access to the internet supports educational and cultural exchanges between students world - wide and enables pupils to participate in cultural, vocational, social and leisure use in libraries, clubs and at home.

4.3 The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data with the Local Authority and DFE.

4.4 The internet improves access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, government initiatives.

4.5 The internet offers opportunities for mentoring pupils and providing peer support for them and their teachers.

4.6 Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of the children and young people.

4.7 Children and young people will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

4.8 Children and young people will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information. Children and young people will also be taught that copying material is worth little without an appropriate commentary demonstrating the selectivity used and evaluating the material's significance.

4.9 Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

5 Managing Internet Access

5.1 Developing good practice in internet use as a tool for teaching and learning is essential. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children and young people.

5.2 Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupil's age and maturity.

5.3 Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening and instructed to report any suspicious use of the internet and digital devices

5.4 If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Co-ordinator.

5.5 The school will ensure that the use of Internet derived materials by staff and pupil complies with copyright law.

5.6 Pupils will be taught to be critically aware of the materials they read as well as how to validate information before accepting its validity.

5.7 All users in KS2 will be provided with usernames and passwords and are advised to keep these confidential to avoid any other pupils or family members attending the school using their log in details.

5.8 A record will be kept of all pupil login details, and this will be updated on the departure or arrival of pupils.

5.9 Any requests to add access to specific websites must first be authorised by the Headteacher

5.10 All school systems will be protected by up to date virus software

6 Managing E-Mail

6.1 Personal e-mail or messaging between staff and pupils should not take place.

6.2 Pupils and staff may only use approved e-mail accounts on the school system and pupils must inform a member of staff immediately if they receive an offensive e-mail.

6.3 Pupils must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.

6.4 Access in school to external personal e-mail accounts may be blocked.

6.5 Excessive social e-mail use can interfere with learning and will be restricted.

6.6 The forwarding of chain letters is not permitted.

6.7 Incoming e-mail should be monitored and attachments should not be opened unless the author is known.

7 Managing Website Content and Twitter Account

7.1 The school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

7.2 Photographs of pupils will not be used without the written consent of the pupil's parents/carers.

7.3 The point of contact on the school website will be the school address, school e-mail and telephone number. Staff, governor or pupil's home information will not be published.

7.4 The Headteacher or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate.

7.5 The website will comply with the school's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing.

7.6 Use of site photographs will be carefully selected so that any pupils cannot be identified or their image misused. Staff must not use their personal equipment to take any photographs of pupils.

7.7 The names of pupils will not be used on the website, particularly in association with any photographs.

7.8 The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

7.9 Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

8 Social Networking and Chat Rooms

8.1 The school will control access to moderated social networking sites and educate pupils in their safe use.

8.2 Pupils will not be able access social networking sites eg 'Twitter', 'Instagram, 'Facebook' or Snapchat'.

8.3 Pupils will be taught the importance of personal safety when using social networking sites and chat rooms and the implications of posting personal information online outside of school.

8.4 Pupils will not be allowed to access public or unregulated chat rooms.

8.5 Pupils will only be allowed to use regulated educational chat environments and use will be supervised.

8.6 Newsgroups will be blocked unless an educational need can be demonstrated.

8.7 Pupils will be advised to use nicknames and avatars when using social networking sites.

8.8 Staff will not exchange social networking addresses or use social networking sites to communicate with pupils or publish comments about the school which may affect its reputability.

9 Mobile Phones and Hand Held Devices

9.1 Mobile phones will not be used during lessons or formal times in school. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden and will be dealt with in accordance with the school's Anti-Bullying and Behaviour Policies.

9.2 Pupils must leave their mobile phones in the school office each morning to be collected at the end of the school day.

9.3 Staff will be issued with a school mobile phone where contact with pupils is necessary or where mobile phones are used to photograph school activities involving pupils.

10 Filtering

10.1 The school will work in partnership with parents/carers and the Internet Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly.

10.2 If staff or pupils discover unsuitable sites, the URL **(address)** and content must be reported to the Headteacher.

10.3 Any material the school deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwf.org.uk).

10.4 Regular checks by Senior Staff will ensure that the filtering methods selected are appropriate, effective and reasonable.

10.5 Filtering methods will be selected by the school in conjunction with the schools service provider and will be age and curriculum appropriate.

11 Authorising Internet Access

11.1 All staff must read and sign the school's 'Staff Code of Conduct for ICT' before using any school ICT resources and any staff not directly employed by the school will be asked to sign the school's 'Acceptable Use of ICT Resources' document before being allowed internet access from the school site.

11.2 The school will maintain a current record of all staff and pupils who are allowed access to the school's ICT systems.

11.3 Staff will supervise access to the internet from the school site for all pupils.

11.4 KS2 pupils will all sign a copy of the 'Acceptable Use Agreement KS2' document.

12 Photographic, Video and Audio Technology

12.1 It is not appropriate to use photographic or video technology in changing rooms or toilets.

12.2 Staff may use photographic or video technology to capture to support school trips and appropriate curriculum activities.

12.3 Audio and video files may not be downloaded without the prior permission of the Headteacher.

12.4 Pupils must have permission from a member of staff before making or answering a video conference call or making a video or audio recording in school or on educational activities.

12.5 Video conferencing and webcam use will be appropriately supervised for the pupil's age.

13 Assessing Risks

13.1 Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The senior leadership team should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

13.2 In common with other media such as magazines, books and video, some material available through the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of Internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

13.3 Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in school is allowed and methods to identify, assess and minimise risks will be reviewed regularly.

13.4 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

13.5 The Headteacher will ensure that the E-Learning Safety Policy is implemented and compliance with the policy is monitored.

13.6 Access to any websites involving gambling, games or financial scams is strictly forbidden and will be dealt with accordingly.

14 Introducing the Policy to Pupils

14.1 Rules for Internet access will be posted in all rooms where computers / Learnpads are used.

14.2 Responsible Internet use, covering both school and home use, will be included in the curriculum.

14.3 Pupils will be instructed in responsible and safe use before being allowed access to the internet and will be reminded of the rules and risks before any lesson using the Internet.

14.4 Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.

15 Consulting Staff

15.1 It is essential that teachers and learning support staff are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies:

- All staff are governed by the terms of the school's 'Staff Code of Conduct for ICT'.
- All new staff will be given a copy of the policy during their induction.
- Staff development in safe and responsible use of the internet will be provided as required.
- Staff will be aware that internet use will be monitored and traced to the original user. Discretion and professional conduct is essential.

16 Maintaining ICT Security

16.1 Personal data sent over the network will be encrypted, password protected or otherwise secured.

16.2 Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mails.

16.3 The ICT Provider will ensure that the system has the capacity to deal with increase traffic caused by internet use.

16.4 Passwords should be changed frequently to ensure maximum security

17 Dealing with Complaints

17.1 The school's designated person for e-safety will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the Headteacher immediately.

17.2 Pupils and parents/carers will be informed of the complaints procedure.

17.3 Parents/carers and pupils will work in partnership with the school staff to resolve any issues.

17.4 There may be occasions when the school must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.

17.5 Sanctions for misuse may include any or all of the following:

- Interview/counselling by an appropriate member of staff
- Informing parents/carers
- Removal of internet access for a specified period of time, which may ultimately prevent access to files held on the system, including examination coursework.
- Referral to the police.

17.6 Concerns relating to safeguarding issues must be dealt with through the school's Safeguarding Policy

17.7 Any complaint must be reported to the Headteacher or Designated Safeguarding Lead immediately.

18 Parents/Carers Support

18.1 Any issues concerning the internet will be handled sensitively to inform parents/cares without undue alarm.

18.2 Advice on filtering systems and appropriate educational and leisure activities including responsible use of the Internet will be made available to parents/carers via the school website. The organisation Child Exploitation and Online Protection (CEOP) can provide information for parents.

18.3 A partnership approach will be encouraged with parents/carers and this may include practical sessions as well as suggestions for safe internet use at home.

19 Community Use

19.1 School ICT resources may be increasingly used as part of the extended school agenda.

19.2 Adult users will sign the school's acceptable use policy.

19.3 Parents/carers of children and young people under 16 years of age will be required to sign the acceptable use policy on behalf of their child.

20 Monitoring and Review

This policy will be reviewed on a bi- annual basis by the Headteacher. Members of staff are required to familiarise themselves with this policy as part of their induction process.