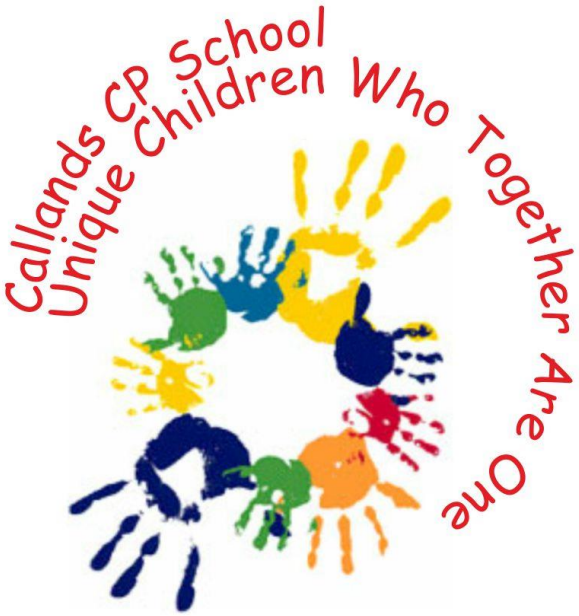

ACCEPTABLE USE POLICY

Adopted by the Governing Body on _____

COG _____

Introduction to Acceptable Use Policy

It is the responsibility of all users of the Organisation I.T. services to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

1.1 Purpose

This Acceptable Use Policy is intended to provide a framework for use of the Organisation's I.T. resources. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

1.2 Policy

This Acceptable Use Policy is taken to include the JANET Acceptable Use Policy and the JANET Security Policy published by JANET (UK), the Combined Higher Education Software Team (CHEST) User Obligations, together with its associated Copyright Acknowledgement, and the Eduserv General Terms of Service. The Organisation also has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed “PREVENT”. The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

1.3 Scope

Members of the Organisation and all other users (staff, students, visitors, contractors and others) of the Organisation's facilities are bound by the provisions of its policies in addition to this Acceptable Use Policy. The Organisation seeks to promote and facilitate the positive and extensive use of Information Technology in the interests of supporting the delivery of learning, teaching, and innovation to the highest possible standards. This also requires appropriate and legal use of the technologies and facilities made available to students, staff and partners of the Organisation.

1.4 Control of Data

Information must be retained under the control of the Organisation at all times. You are not authorised to copy any data to any other device other than storage provided by the Organisation, including, but not limited to, local drives, USB Sticks (unless provided by the Organisation and encrypted) and remote document storage areas. Where information is synchronised to another device you must inform us and enter into an agreement for its remote deletion. You must not take photographs except using equipment provided by the Organisation, and any images must be immediately deleted after uploading to the controlled environment. Sensitive data should not be sent by email unless encryption is used and wherever possible names should be anonymised.

2 Unacceptable Uses

a) The Organisation Network may not be used directly or indirectly by a User for the download, creation, manipulation, transmission or storage of:

1. any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
2. unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
3. unsolicited “nuisance” emails;
4. material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the Organisation or a third party;
5. material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;
6. material with the intent to defraud or which is likely to deceive a third party;
7. material which advocates or promotes any unlawful act;
8. material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or
9. material that brings the Organisation into disrepute.

b) The Organisation Network must not be deliberately used by a User for activities having, or likely to have, any of the following characteristics:

1. intentionally wasting staff effort or other Organisation resources;
2. corrupting, altering or destroying another User’s data without their consent;
3. disrupting the work of other Users or the correct functioning of the Organisation Network; or
4. Denying access to the Organisation Network and its services to other users.

c) Any breach of industry good practice that is likely to damage the reputation of the JANET (or other) network will also be regarded prima facie as unacceptable use of the Organisation Network.

d) Where the Organisation Network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the Organisation Network.

e) Users shall not:

1. introduce data-interception, password-detecting or similar software or devices to the Organisation’s Network;
2. seek to gain unauthorised access to restricted areas of the Organisation’s Network;
3. access or try to access data where the user knows or ought to know that they should have no access;
4. carry out any hacking activities; or
5. Intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

3 Consequences of Breach

In the event of a breach of this Acceptable Use Policy by a User the Organisation may in its sole discretion:

a) Restrict or terminate a User's right to use the Organisation Network;

b) Withdraw or remove any material uploaded by that User in contravention of this Policy; or

c) Where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.

In addition, where the User is also a member of the Organisation community, the Organisation may take such action, disciplinary or otherwise as it deems appropriate and which is in accordance with its Charter, Statute, Ordinances and Regulations.

4 Definitions

Organisation Network – all computing, telecommunication, and networking facilities provided by the Organisation, with particular reference to all computing devices, either personal or Organisation owned, connected to systems and services supplied.

IT Acceptable Use Policy

1. The aim of this policy is to ensure that Callands Community Primary School IT facilities are used: safely, lawfully and equitably.

2. Callands Community Primary School seeks to promote and facilitate the proper and extensive use of Information Technology in the interests of learning, teaching and research, including business and community engagement partnerships. Whilst the tradition of academic freedom will be fully respected, this also requires responsible and legal use of the technologies and facilities made available to students, staff and partners of Callands Community Primary School.

3. This Acceptable Use Policy is intended to provide a framework for such use of Callands Community Primary School's I.T. resources. It applies to all computing, telecommunication, and networking facilities provided at Callands Community Primary School. It should be interpreted such that it has the widest application, in particular references to I.T. Services should, where appropriate, be taken to include departmental or other system managers responsible for the provision of an I.T. Service. This policy should be interpreted so as to encompass new and developing technologies and uses, which may not be explicitly referred to.

4. Users of commercial broadband services provided, or facilitated by, Callands Community Primary School must abide by any specific policies associated with those services. Members of Callands Community Primary School and all other users of the School's facilities are bound by the provisions of these policies in addition to this Acceptable Use Policy. They are also bound by such other policies as are published via Callands Community Primary School on the IT Services policies website. It is the responsibility of all users of Callands Community Primary School's I.T. services to read and understand this policy.

Scope

5. This policy applies to anyone using School IT facilities (hardware, software, data, network access, telephony, services provided by licensed third parties, online cloud services or using School IT credentials) including students, staff, tenants and third party individuals who have been given access for specific purposes. The term School IT facilities refers to all IT facilities**;** whether they are provided**,** or arranged**,** by IT Services**,** or by Schools**,** or by other Professional Services. It is the responsibility of all users of Callands Community Primary School's IT facilities to read, understand and comply with this policy and any additional policies related to their activities, including other relevant information security policies.

6. This policy is issued under the authority of the Information Technology and Governance Committee. Responsibility for their interpretation and enforcement is delegated to IT Services and School IT Professionals.

7. You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of this policy. If you feel that any such instructions are unreasonable or are not in support of this policy, you may appeal to the Director of IT Services.

Acceptable Use

8. School IT resources are provided primarily for academic and operational purposes to support learning and teaching, research, enterprise and the other work of Callands Community Primary School. Facilities are also provided to students to enhance their wider experience at the School.

9. Whilst the principles of academic freedom will be fully respected, facilities must only be used responsibly, in accordance with the law and not to bring Callands Community Primary School into disrepute.

10. School IT facilities may be accessed via School owned devices or via personally owned devices but this policy is applicable, regardless of the ownership of the device used. Personally owned devices whether owned by students or staff must be maintained with up to date anti-virus software (where appropriate), system patches and kept secure in accordance with the Mobile Working Policy (link). Devices provided to staff by Callands Community Primary School for their personal use must also be kept secure in a similar manner.

11. Use of the facilities for personal activities is permitted, provided that it does not infringe the law or School policies, does not interfere with others' valid use and, for staff, is not done inappropriately during their working hours. However, this is a privilege that may be withdrawn by the Director of IT Services, at any point, if such use is not in accordance with this policy.

12. Using School owned or managed services for commercial work for outside bodies, that is being undertaken on a personal basis, solely for personal gain and not through School channels, requires explicit permission from the Director of IT Services.

13. School e-mail addresses and associated systems, must be used for all official School business, in order to facilitate auditability and institutional record keeping. All staff and students of Callands Community Primary School must regularly read their School e-mail.

14. When using the Callands Community Primary School's IT facilities, you remain subject to all relevant laws and policies, and, when accessing services from another legal jurisdiction, you must abide by all relevant local laws, as well as those applicable to the location of the service. Following the requirements of this policy, and other School policies and procedures applicable to your activities, should normally ensure that you comply with the law. However, if you have any concerns about whether planned actions might be regarded as unlawful please contact the Headteacher for further advice.

15. You must abide by the policies and terms & conditions applicable to any other organisation whose services you access. When using School IT services from another partner institution, you are subject to both Callands Community Primary School's requirements and those of the institution where you are accessing services.

16. Users must adhere to any licence conditions when using software procured by Callands Community Primary School. If you use any software or resources covered by a Chest agreement, you are deemed to have accepted the Eduserv User Acknowledgement of Third Party Rights.

17. Further details of what constitutes acceptable and unacceptable use is provided in the subsequent sections of this policy.

Keeping Your IT Credentials Secure

18. You must take all reasonable precautions to safeguard your username, password and any other IT credentials issued to you. Advice is available on the choice of passwords . You must not allow anyone else to use your IT credentials. No-one has the authority to ask you for your password, and you must not disclose it to anyone, including the IT Service Desk.

19. You must not attempt to obtain or use anyone else's credentials; and you will be held responsible for all activities undertaken using your IT credentials including access through the Hallnet Service. You should only use the access to School systems provided to you under the Management of User Access Policy for the purpose which that access was granted.

20. You must not impersonate someone else or otherwise disguise your identity when using the IT facilities.

Safeguarding of Information

21. You must make yourself aware of the Callands Community Primary School's Information Categories and Controls Policy and take all reasonable steps to safeguard any information you have access to in accordance with the law (Data Protection Act) and the Callands Community Primary School's information security policies for staff and students.

22. You must not infringe copyright, or break the terms of licences for software or other material.

23. You should ensure you are aware of the appropriate procedures for handling any Confidential or Highly Confidential School information to which you have access. Sharing of this information should only be undertaken in accordance with the Callands Community Primary School's [Information Sharing] policy. You must not attempt to access, delete, modify or disclose information belonging to other people without their permission, or explicit approval from the Director if IT (or nominee) or Director of HR (or nominee).

24. You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening or discriminatory. In the event that there is a genuine academic need to carry out an activity which might be interpreted as being in breach of the law (e.g. the deliberate viewing or accessing of sites or media which are specifically designed to promote terrorism or which are directly linked to a proscribed terrorist organisation), Callands Community Primary School must be made aware of your plans in advance and prior permission to access must be obtained from the Headteacher.

Behaviour

25. The conduct of staff and students when using the Callands Community Primary School's IT facilities should always be in line with the School's values, including the use of online and social networking platforms. When using School IT facilities, you must not:

a. cause needless offence, concern or annoyance to others including posting of inappropriate comments about students or members of staff (genuine scholarly criticism and debate is acceptable);

b. use the IT facilities in a way that interferes with others' valid use of them;

c. undertake any illegal activity including the downloading and storing of: copyright information, except under a relevant licence, or with permission from the copyright owner;

d. view, store or print pornographic images or video;

e. the retention or propagation of sites or media which are specifically designed to promote terrorism or which are directly linked to a proscribed terrorist organisation, except in the course of recognised research or teaching that is permitted under UK and international law;

f. send spam (unsolicited bulk email), forge addresses, or use School mailing lists other than for legitimate purposes related to School activities;

g. deliberately or recklessly consume excessive IT resources such as processing power, bandwidth, storage or consumables;

h. undertake any activity which jeopardises the security, integrity, performance or reliability of electronic devices, computer equipment, software, data and other stored information. This includes undertaking any unauthorised penetration testing or vulnerability scanning or the monitoring or interception of network traffic, without permission;

i. deliberately or recklessly introduce malware or viruses;

j. attempt to disrupt or circumvent IT security measures.

26. WiFi and other ICT equipment and services provided for private use.

a. When using WiFi provided by Callands Community Primary School for use with personally-owned devices, or other IT provided specifically for private use, always follow any Terms and Conditions. The section above – 'Behaviour' – applies (it will help you stay within the law).

<u>Monitoring</u>

27. School records and monitors the use of its IT facilities, under the Regulation of Investigatory Powers Act (2000) for the purposes of:

a. The effective and efficient planning and operation of the IT facilities;

b. Investigation, detection and prevention of infringement of the law, this policy or other School policies;

c. Investigation of alleged misconduct by staff or students;

28. School will comply with lawful requests for information from government and law enforcement agencies.

29. You must not attempt to monitor the use of the IT facilities without explicit authority to do so.

30. Access to workspaces, email, and/or individual IT usage information will not normally be given to another member of staff unless authorised by the Director of IT, or nominee, who will use their discretion, normally in consultation with the Director of Human Resources or other senior officer of Callands Community Primary School.

31. Where there is a requirement to access the account of another member of staff, Head of Professional Service should contact the IT Service desk with the circumstances.

32. If the request for access is related to a HR investigation, this should be managed wholly through the HR advisor who will work with IT if approved by the Director of Human Resources or their nominee.

Implementation and Enforcement of this Policy

33. This policy is issued under the authority of the Information Technology and Governance Committee. Responsibility for its interpretation and enforcement is delegated to IT Services, IT Professionals and the Academic Registry by the Chief Operating Officer.

34. You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of the implementation of this policy. If you feel that any such instructions are unreasonable or are not in support of this policy, you may make a complaint under the relevant staff or student procedures.

35. If you believe this policy has been infringed, you should report the matter to the Headteacher, overseen by IT Services, at the earliest opportunity. Follow up action will be considered carefully. Genuinely accidental infringement will be treated with understanding but any deliberate or wilfully negligent infringement of this policy is likely to result in disciplinary action being taken under the relevant School Ordinance

36. Penalties may include withdrawal of services and/or fines. Offending material will be taken down.

37. Information about deliberate infringement or illegal activities may be passed to appropriate law enforcement agencies, and any other organisations whose requirements you may have breached.

38. School reserves the right to recover from you any costs incurred as a result of your infringement.

Further Information

39. The user must comply with all relevant legislation and legal precedent, including the provisions of the following specifically related Acts of Parliament, or any re-enactment thereof:

- Malicious Communications Act 1988
- Computer Misuse Act 1990
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Investigatory Powers Act 2016
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

- Communications Act 2003
- Counter-Terrorism and Security Act (2015)