IT and Communications Systems Policy incorporating:

Roles and Responsibilities

Digital and Technology Standards including filtering and monitoring

Online Safety

Social Media

Use of personal devices (staff and pupils)

Digital Images

Video Conferencing and Live Stream / Remote Learning

Loan of Equipment Agreement

Acceptable Use Agreement

Pupil and Parent Code of Conduct for livestream learning

Remote Learning Livestream Log

Video Conferencing – good practice

This policy has undergone an Equalities Impact Assessment in line with the requirements of the Public Sector Equality Duty

Committee:	Trust Board
Policy Ratified:	October 2026
Review Date:	October 2027

Additional School Procedure – N/A	
Committee:	
Procedure Adopted:	
Review Date:	

Table of Contents

Part One: Roles and Responsibilities 4
1 The Trust Board 4
2 The Local Governing Body 4
3 The Head of Operations 5
4 The Chief Finance Officer 6
5 Headteacher and Senior Central Leaders 6
6 Online Safety Champions 7
7 Teaching and pupil facing Staff 9
8 Designated Safeguarding Leads 9
9 ICT Technicians and ICT Network Providers 10
10 The Head of HR 10
11 All Staff including Governors and Trustees, agency staff, volunteers and consultants working in schools or remotely for the Trust 11
12 Parents / Carers 11
13 Visitors and members of the community 12
Part Two: Introduction and General Principles 13
14 About this policy 13
15 The ICT Network 13
16 Equipment security and login credentials 15
17 Systems and data security 17
18 Email Security and login credentials 18
19 Using the internet – general principles 20
20 Personal use of the ICT network and our systems 20
21 Monitoring 21
22 Prohibited use of our systems 21
23 Use of Personal mobile, smart technology and cloud accounts – staff, Governors/Trustees, agency staff, volunteers and consultants (also known as Bring Your Own Device BYOD) 22
24 Use of Personal mobile and smart technology – pupils (also known as Bring Your Own Device BYOD) 24
25 Acceptable Use Agreements (AUAs) and issues of misuse 26
26 Equipment Loaned to Pupils 27
27 New Technologies 27
28 Online Safety 27
29 Education – parents / carers 28
30 Education & Training – Teaching Staff, Volunteers and Governors 28
31 Digital Images 28
32 Taking and use of images 29
33 Social Media and Private Messaging Applications / Software 30
34 Use of Social Media and Private Messaging Applications in practice 30
35 Personal Use of Social Media and Private Messaging Applications 31

36 Approved business and professional use of social media 31
37 Pupils' use of social media 32
38 Video Conferencing and Live Stream Remote Working 32
39 Approved use of video conferencing for professional and business use 33
40 Live Stream Remote Learning 34
41 Generative artificial intelligence (AI) in education 35
Appendix A: Loan of Equipment Agreement 36
Appendix B: Loan of Equipment to Pupils letter template 38
Appendix C: Acceptable Use Agreements 39
Appendix D: Pupil, Parent and Carer Code of Conduct for livestream learning 44
Appendix E: Video Conferencing - good practice 45
Appendix F: CLP ICT Network Key Contacts 46
Appendix G: CLP Core Systems Matrix 47
Appendix H: External disclaimer 49
Appendix I: Use of What's App for work purposes 50

Part One: Roles and Responsibilities

1 The Trust Board

1.1 The Trust Board recognises its responsibility for ensuring that sufficient resources are in place to enable the provision and development of IT and communications systems so that its schools and employees can deliver effectively the Partnership's education and business aspirations.

1.2 The Trust Board is responsible for the approval of this Policy; Local Governing Bodies (LGBs) are responsible for ensuring that schools are meeting the requirements of the policy.

1.3 The Trust Board will:

1.3.1 Review annually the Partnership's overall strategy (including infrastructure such as ICT) and receive for annual approval the Capital Investment Plan (to include ICT).

1.3.2 Require annual reporting to the Resources Committee on ICT infrastructure in accordance with the CLP Reporting Framework.

1.3.3 Have due regard to cyber security and online safety provision as required by the Academies Trust Handbook[1], Keeping Children Safe in Education[2] and Meeting digital and technology standards in schools and colleges[3] ensuring that adequate resources for implementation and training are made available.

1.3.4 Appoint a Digital and Technology Standards[4] responsible trustee who will work closely with the Head of Operations to monitor implementation of this policy and provide support.

1.3.5 Ensure a Designated Safeguarding Lead is appointed to undertake the annual review of filtering and monitoring arrangements.

1.3.6 Annually review the IT strategy and compliance with Digital and Technology Standards.

1.4 Annually and as required review the effectiveness of the policy and ensure that any necessary changes are made. The annual review should align with the annual Keeping Safe Children in Education update.

2 The Local Governing Body

2.1 The LGB has responsibility for monitoring the implementation of this policy in their school and will meet with key staff to discharge this duty.

2.2 The LGB will:

2.2.1 Ensure that ICT is properly considered in the school's improvement planning cycles.

2.2.2 Ensure the Headteacher allocates sufficient resources to support the delivery of the school's IT improvement needs.

2.2.3 Nominate a lead governor for Safeguarding, to include online safety, who will take part in online safety training awareness sessions arranged by the school's Online Safety Champion.

---

[1] https://www.gov.uk/guidance/academy-trust-handbook
[2] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
[3] Meeting digital and technology standards in schools and colleges
[4] Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK

3 The Head of Operations

3.1 The Head of Operations:

3.2 Has overall responsibility for the effective operation of this policy and for ensuring compliance across the Partnership, for reviewing effectiveness of the policy, ensuring periodic review and reporting to the CEO and Trust Board, for monitoring compliance and reporting non-compliance.

3.3 Is responsible for ensuring an independent network audit is undertaken annually.

3.4 Is responsible for provision of asset management across the Partnership ensuring an accurate asset register is maintained and:

3.4.1 All new equipment is added.

3.4.2 Equipment is allocated to users and locations.

3.4.3 All unwanted equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) Regulations and the Data Protection Act 2018, and the Finance Regulation Manual.

3.5 Is responsible for the appointment of professional IT services.

3.6 The Head of Operations is responsible for ensuring:

3.6.1 The ICT network defined in paragraph 15.1 is secure and not open to misuse or malicious attack.

3.6.2 That all users can only access the ICT network and Partnership equipment through a properly enforced profile and login credentials protection policy.

3.6.3 Adequate Content filtering, backup, virus protection and monitoring as required by Keeping Children Safe in Education and specified in Meeting digital and technology standards in schools and colleges and Part Two of this policy is in place across the network and that implementation is not the sole responsibility of any single person.

3.6.4 The use of the network / internet / virtual learning environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be identified and reported.

3.6.5 The investigation of IT security related incidents.

3.6.6 The monitoring of computer user activity in support of investigations into breaches of this policy, when and where required.

3.6.7 Reporting findings to the HR Team and/or relevant Senior Leaders.

3.7 The Head of Operations will:

3.7.1 Keep up to date with technical information in order to effectively carry out their role and to inform and update others as relevant.

3.7.2 Provide advice to all users regarding implementation of this policy as required.

3.7.3 Provide support and guidance to employed IT Technicians by challenging where necessary, providing learning opportunities and facilitating networking.

3.7.4 Ensure filtering reporting arrangements are in place to enable the Designated Safeguarding Leads to fulfil their obligations in Keeping Children Safe in Education and provide support in interpreting reports.

3.7.5 Undertake and coordinate an annual review of filtering and monitoring arrangements with the Partnership and school Designated Safeguarding Leads as required by Keeping Children Safe in Education.

3.7.6 Make recommendations on the development of the ICT network.

3.7.7 Coordinate with the professional IT service provider to undertake business continuity and disaster management scenarios and practice.

3.7.8 Ensure a Cyber Response Plan aligned to NCSC and the Digital and Technology Standards is in place.

4 The Chief Finance Officer

4.1 The Chief Finance and Operations Officer:

4.2 Is responsible for provision of adequate resources to enable arrangements required by this policy, the Academies Trust Handbook, Keeping Children Safe in Education and [5]Meeting digital and technology standards in schools and colleges.

4.3 Is responsible for ensuring that the Head of Operations receives adequate resources to enable them to carry out their role, specifically to put requirements at 15.2 in place.

5 Headteacher and Senior Central Leaders

5.1 In this section, these people will be referred to **as Senior Leaders** and they have delegated responsibility for ensuring all users, contractors and other visitors on their site operate within the policy. For clarity, in relation to this policy the central offices are treated as a school and scope of responsibility of Senior Leaders is:

5.1.1 Headteacher – their school including all staff and visitors to their school.

5.1.2 Senior Central Leaders – their staff and all visitors to the central offices.

5.2 **All Senior Leaders** (Headteachers and Senior Central Leaders) **must** ensure:

5.2.1 All staff who report to them, read and adhere to this policy.

5.2.2 Agency staff, consultants and volunteers who they engage have an understanding of this policy and its requirements and:

(a) That these people are not allocated employee access to equipment, email and the ICT network without relevant disclaimers being signed.

(b) That the use of generic email and ICT network access is not recommended practice but if put in place that a log is maintained as per 18.9.

5.2.3 In the event of a serious online safety allegation being made against a member of staff Senior Leaders **must** liaise with the HR Team. It may also be relevant to inform the Head of Operations so a review of controls and monitoring can be coordinated.

5.2.4 The Head of Operations and relevant ICT Network provider is quickly informed of all suspected virus or malware attack or IT security related incidents.

5.2.5 They remind all staff who report to them of this policy and its expectations annually.

[5] https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges

5.2.6 That policy queries and development needs are raised with the Head of Operations at the earliest opportunity.

5.2.7 That they and their staff support the Head of Operations in the implementation of this policy and the network requirements defined in paragraph 15.2, and make information readily made available to the Head of Operations and IT Service Provider as necessary.

5.2.8 That all staff are aware of the need to maintain an accurate asset register and of the arrangement put in place by the Head of Operations.

5.2.9 That all staff who report to them complete **Appendix A: Loan of Equipment Agreement** for any items taken off site.

5.2.10 That all staff and all those with a governance responsibility complete **Appendix C: Acceptable Use Agreements** annually.

5.2.11 A log of all social media accounts within their area of responsibility as defined in 4.1 is maintained.

5.2.12 A log of all generic email and network profile accounts is maintained and that these accounts are signed for before each use. From time to time these logs will need to be made available to the Head of Operations for audit.

5.2.13 Personal device expectations are clearly displayed at point of sign in (NB. The use of personal devices in schools must not be prohibited but managed carefully to avoid safeguarding risks).

5.3 In addition, **Headteachers** are responsible for ensuring:

5.3.1 An Online Safety Champion is appointed, and:

(a) That the LGB is informed of this appointment each year.

(b) That they receive suitable training to enable them to carry out their role and to train the school community as required by Keeping Children Safe in Education and by this policy.

(c) That they are named on the school's Online Safety website page.

5.3.2 That they work with the Online Safety Champion and Designated Safeguarding Lead to ensure that the school's behaviour policy adequately reflects awareness of bullying and other inappropriate behaviour through the use of digital and smart technology as required by Keeping Children Safe in Education paragraph 137[6]. In doing so they must have consideration for the expectations and standards set out in Section 24 of this policy with regards to the use of mobile and smart technology.

5.3.3 That pupils and parents complete the **Acceptable User Agreements at Appendix C** annually.

6 Online Safety Champions

6.1 The Online Safety Champion is responsible for:

6.1.1 Reading and understand the requirements of Keeping Children Safe in Education with specific regard to online safety.

6.1.2 Ensuring they receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

[6] Keeping children safe in education 2025

6.1.3 Establishing and reviewing online safety procedures and documents used in their school to ensure these are up to date and relevant to current technologies and risks.

6.1.4 Promoting online safety generally throughout the school community including ensuring that pupils and parents understand the expectations and standards set out in Section 24 of this policy.

6.1.5 Acting as an immediate point of contact for any member of staff or pupil who may have an immediate concern related to online safety and ensuring that all staff are aware of the procedures that need to be followed in the event of an online incident taking place.

6.1.6 Providing training opportunities and guidance for the school community, including staff, parents and carers and governors as outlined in Part Two sections 29/30 of this policy.

6.1.7 Providing regular updates on online safety in school to the Headteacher and local governing body.

6.1.8 Working closely with the school Designated Safeguarding Lead to ensure online arrangements are contributing effectively to overall safeguarding arrangements in the school including:

(a) Cyberbullying controls

(b) Online harassment reporting

(c) Harmful content risks

(d) Misinformation

6.1.9 Reporting online safety incidents to the Headteacher, Governors and the Head of Operations to inform reporting and enable issues and vulnerabilities to be addressed and make provision for future developments.

6.2 Specifically with regard to parents and carers, the Online Safety Champion will:

6.2.1 Take every opportunity to help parents understand online safety issues through parents' evenings, newsletters, letters, curriculum activities and by providing information about national and local online safety campaigns.

6.2.2 Provide online safety information for parents and carers, and the wider community, on the school website.

6.2.3 Provide or facilitate family learning courses in use of new digital technologies, digital literacy and online safety.

6.3 Specifically with regard to staff, the Online Safety Champion will provide or facilitate the following:

6.3.1 An annual update to all staff on the general principles of online safety during which this policy will be referred to.

6.3.2 Additional training, advice and guidance as required.

6.3.3 Online Safety training to new teaching staff as part of their induction programme, ensuring that they are made aware of this policy and the importance of adhering to it.

6.3.4 Ensure that staff know how to report online material promoting terrorism or extremism[7].

[7] https://www.gov.uk/report-terrorism

7 Teaching and pupil facing Staff

7.1 Teaching and support staff working with pupils are responsible for ensuring:

7.1.1 All digital communications with students, pupils, parents and carers are on a professional level and only carried out in line with Keeping Children Safe in Education and this policy.

7.1.2 Online safety is embedded in all aspects of the curriculum and other activities.

7.1.3 Pupils understand and follow online safety guidelines.

7.1.4 They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement safeguards with regard to these devices.

7.1.5 In lessons where internet is used, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

7.1.6 They are vigilant to pupils possessing mobile and smart technology devices – section 24 refers.

8 Designated Safeguarding Leads

8.1 Designated Safeguarding Leads will read and understand the requirements of Keeping Children Safe in Education and, for the purposes of this policy, with specific regard to online safety, filtering and monitoring, and the use of mobile and smart technology.

8.2 Designated Safeguarding Leads **must** have a good awareness of the potential for serious child protection / safeguarding issues to arise from:

8.2.1 Sharing of personal data.

8.2.2 Access to illegal / inappropriate materials.

8.2.3 Inappropriate on-line contact with adults / strangers.

8.2.4 Potential or actual incidents of grooming.

8.2.5 Cyber-bullying.

8.3 Designated Safeguarding Leads will work closely with the Online Safety Champions and in particular will:

8.3.1 Ensure that online safety arrangements are effective in their contribution to overall safeguarding arrangements.

8.3.2 Ensure that pupils and parents understand the expectations and standards set out in Section 24 of this policy.

8.3.3 Work with the Headteacher, ICT Coordinator (or equivalent) and other staff, as necessary, to address any online safety issues or incidents.

8.3.4 Ensure that any online safety incidents are recorded and dealt with appropriately in line with this policy and other linked policies and that procedures are in place for handling attempted access to harmful content.

8.3.5 Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.

8.3.6 Consider whether an incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

8.4 Designated Safeguarding Leads will work closely with the Head of Operations and in particular will:

8.4.1 Understand arrangements for filtering and monitoring and know how to access support with regards to arrangements and reporting.

8.4.2 Receive and monitor filtering reporting, ensuring that concerns are raised as appropriate and as detailed in the CLP Safeguarding and Child Protection Policy.

8.4.3 Contribute to the annual review of filtering and monitoring arrangements, including reporting arrangements.

9 ICT Technicians and ICT Network Providers

9.1 It is recognised that some schools will employ an ICT Technician who has a limited level of responsibility for network management. In the course of maintaining their local network and equipment these individuals **must** comply with this policy and ensure that they share critical information about their school network with the ICT provider to ensure business continuity in the event of their absence. Overall accountability and management of the ICT network lies with the appointed professional IT services provider.

9.2 The appointed IT professional services provider **must**:

9.2.1 Maintain the confidentiality, integrity and availability of the ICT network and systems and the data they contain.

9.2.2 Implement, monitor and, where appropriate, enforce compliance with this policy; in doing so they are required to report concerns, non-compliance and incidents to the **Head of Operations**.

9.2.3 Ensure content filtering backup, virus protection and monitoring as specified in Part Two of this policy is in place across the network and updated on a regular basis and ensure testing and validation of web filtering categories.

9.2.4 Ensure the ICT network, including email, complies with the requirements set out in Part Two of this policy.

9.2.5 Ensure the email disclaimer at 18.3 is deployed on all email accounts.

9.2.6 Ensure technical workflows support the implementation of this policy and other CLP policies including AI, Data Protection and Child Protection and Safeguarding policies.

9.2.7 Work with and respond to information and activity requests from the **Head of Operations**.

9.2.8 Support key staff (Head of Operations, Data Protection Officer, Online Safety Champions, Designated Safeguarding Leads, Headteachers…) in investigating any IT or cyber security related incidents.

10 The Head of HR

10.1 The Head of HR is responsible for:

10.1.1 Ensuring that, as part of their contract of employment and induction, new staff are made aware of and agree to this policy and sign the **Acceptable Use Agreement** at **Appendix C**.

10.1.2 Providing the Head of Operations with a termly list of all staff leavers and changes so that IT systems can be updated and cleansed.

10.1.3 Implementing a Partnership wide induction programme that includes cyber security and online safety.

11 All Staff including Governors and Trustees, agency staff, volunteers and consultants working in schools or remotely for the Trust

11.1 **All** staff, Governors and Trustees, agency staff, volunteers and consultants working in schools or remotely for the Trust, eg, at home, have responsibility for the ICT network, communication systems and data security and will ensure:

11.1.1 Their usernames and passwords or passphrases are used by them alone and not shared.

11.1.2 Their usernames and passwords or passphrases are kept securely and safe.

11.1.3 They do not use another person's username or password or passphrase even if it is offered to them.

11.1.4 Ensure they follow guidance to enable multi factor authentication on their personal work accounts.

11.1.5 They report the loss, theft or damage of any Partnership equipment immediately to a Headteacher or Senior Central Leader.

11.1.6 They have an up-to-date awareness of online safety matters and of this policy.

11.1.7 They report **any** suspected breach of this policy (such as misuse or procedural irregularity or loss of information or inappropriate sharing) or cyber-incident to the Head of Operations or Headteacher or Senior Central Leader or the ICT Service Provider for investigation.

11.1.8 They do not use non-partnership accounts to discuss the personal information of staff, pupils, parents, or of any individual person. Further clarification around the use of text messaging or What's App is provided in Appendix I.

11.1.9 They do not use non-partnership email accounts for any work matters.

11.2 **All** staff, Governors and Trustees, agency staff, volunteers and consultants working in schools or remotely for the Trust are **expected** to:

11.2.1 Be aware of the reporting mechanism for IT incidents or cyber concerns.

11.2.2 Report any breach of this policy or cyber-incident to the Head of Operations or Headteacher or Senior Central Leader or the ICT Service Provider

11.2.3 Cooperate with any subsequent investigation and recommendations.

11.2.4 Agree and adhere to the **Acceptable Use Agreement at Appendix C**.

11.2.5 Read Keeping Children Safe in Education (KCSIE) annually to the extent required of their role as described in the Safeguarding Policy.

12 Parents / Carers

12.1 Parents and carers are expected to:

12.1.1 Notify the school Online Champion or a senior member of staff of any concerns or queries regarding this policy.

12.1.2 Support the school in its endeavours to prevent and resolve any online safety / cyber-bullying incidents.

12.1.3 Discuss the Pupil **Acceptable Use Agreement at Appendix C** with their child and so support the school in underlining the importance of that agreement and ensuring that its content is understood.

12.1.4 Ensure that they have read, understood, signed, returned and adhere to the Parent/Carer **Acceptable Use Agreement at Appendix C**.

13 Visitors and members of the community

13.1 Visitors and members of the community can only use the ICT network and Trust/school equipment with specific permission from a Senior Leader as defined in paragraph 4. Where permission is granted:

13.1.1 They will be made aware of this policy and will be expected to read and follow it.

13.1.2 They should not use a member of staff's network profile.

13.1.3 They will be expected to sign the **Acceptable User Agreement at Appendix C**.

Part Two: Introduction and General Principles

14 About this policy

14.1 Coastal Learning Partnership's IT and communications systems are intended to promote effective communication and working practices within and between our schools. This policy:

14.1.1 Outlines the standards that **must** be observed when using these systems, the circumstances in which we will monitor use, and the action we will take in respect of breaches of these standards.

14.1.2 Applies to all employees, consultants, contractors, service providers, volunteers, interns, casual and supply staff, agency workers and anyone who has access to our IT and communication systems.

14.1.3 Does not form part of any employee's contract of employment and we may amend it or depart from it at any time.

14.1.4 Has due regard to cyber security and online safety requirements set out in the Academies Trust Handbook[8] and Keeping Children Safe in Education[9].

14.2 Related Policies and Documents include:

14.2.1 CLP Safeguarding and Child Protection Policy and Procedures

14.2.2 CLP Data Protection Policy

14.2.3 HR Policies including Code of Conduct, Disciplinary and Anti-Harassment

14.2.4 Equal Opportunities

14.2.5 Privacy Notices

14.2.6 CLP Behaviour and Exclusion Policy

14.2.7 School behaviour policies

14.2.8 CLP Complaints Policy

14.2.9 CLP CCTV Policy

14.2.10 CLP AI Policy

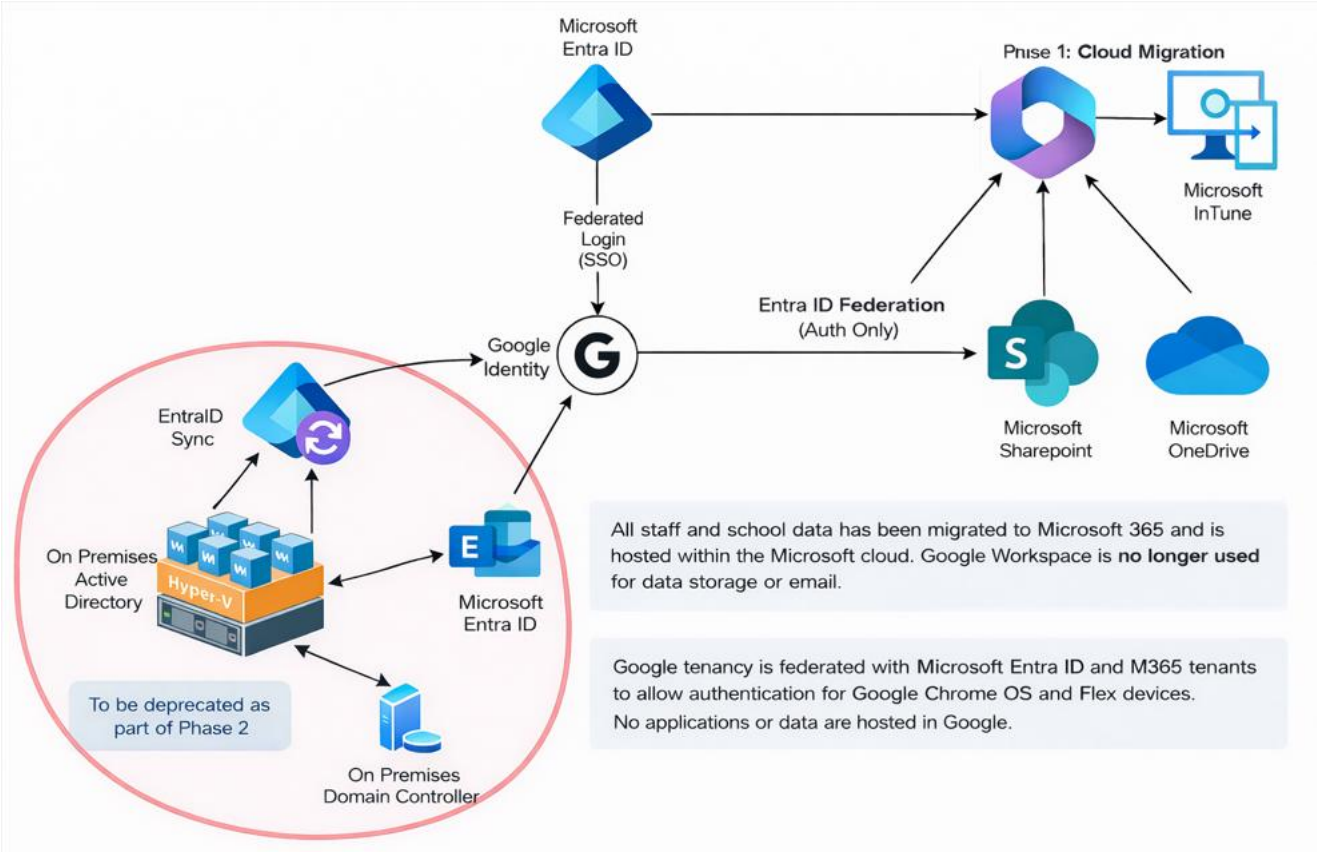
15 The ICT Network

15.1 The Coastal Learning Partnership ICT network is a single trust wide cloud network built on M365 and throughout this policy will be referred to as the ICT network. A legacy Google network has been federated with the M365 platform to enable use of authentication for Google devices; these will be replaced over time so that the network is only M365. No applications or data is stored on Google.

15.2 Systems used by Partnership schools for core activities are listed in **Appendix G**.

15.3 Where schools wish to consider an alternative system, they must follow the Data Protection Impact Assessment process outlined in the Data Protection Policy to ensure that information security and data protection are properly considered.

[8] https://www.gov.uk/guidance/academy-trust-handbook
[9] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2



15.4 As a minimum, the ICT network **must** provide the following in line with Keeping Children Safe in Education and [10]Meeting digital and technology standards in schools and colleges and Generative AI: product safety expectations[11]:

15.4.1 Encrypted offsite backup

15.4.2 Virus and firewall protection

15.4.3 Granular content filtering, including AI content, and reporting

15.4.4 Monitoring

15.4.5 Multi factor authentication (known as 2FA or MFA) **must** be in place on **all** email and online storage accounts used by schools and for all remote and cloud access. To avoid disruption to teaching and Partnership business, multi factor authentication applications will whitelist school IP addresses where possible.

15.4.6 All devices, including iPads and tablets, **must** have device management in place in order to enable encryption and filtering to enable monitoring (in line with Keeping Children Safe in Education) and to ensure operating systems are up to date.

15.4.7 Disaster recovery

15.4.8 Broadband and wireless, including guest broadband for use by non-employees

15.4.9 Cyber security governance

[10] https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges
[11] https://www.gov.uk/government/publications/generative-ai-product-safety-expectations/generative-ai-product-safety-expectations

15.5 Content filtering and monitoring should not result in over blocking leading to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding (Keeping Children Safe in Education paragraph 133).

15.6 Reporting must be provided as agreed with the ICT Network Manager to enable obligations described in Keeping Children Safe in Education to be met.

15.7 The Partnership's management of filtering and monitoring is structured as follows:

15.7.1 The Chief Finance and Operations Officer must ensure funds are available to ensure provision.

15.7.2 The Head of Operations must make arrangements for filtering and monitoring, and reporting, by working with the IT Service Provider and these arrangements must be reviewed annually with the Partnership's Designated Safeguarding Lead.

15.7.3 The IT Service Provider will implement these arrangements and be available to assist with queries and concerns. They must ensure school devices, where technically possible, remain subject to filtering and monitoring controls regardless of location. They will ensure that reports are made available to DSLs and Headteachers through the use of nominated mailboxes to which relevant users are added.

15.7.4 School Designated Safeguarding leads are responsible for reviewing reports and raising concerns either directly to the IT Service Provider (copying in the Head of Operations) or directly with the Head of Operations and for participating in the annual review of arrangements.

15.7.5 The annual review of filtering and monitoring arrangements will take place as part of the Designated Safeguarding Leads forum which meets regularly (at least termly). The Chief Executive Officer, Head of Operations and Designated Safeguarding Leads are all members of this forum.

15.8 The Trust Board will appoint a Trustee to be responsible for filtering and monitoring and cyber security governance, and they will receive reporting as required ensuring the Trust's Risk Register has a focus on cyber security .

15.9 To ensure responsibility for policy implementation and network security does not rest with a single individual, as a minimum there **must** be a half termly external check of any network that forms part of the CLP ICT Network by an appointed provider who, as a minimum, will ensure the integrity of the individual network and that arrangements are in place as per paragraph 15 of this policy. Concerns **must** be reported to the Head of Operations at the earliest opportunity.

15.10 Guest use of the Partnership's internet **must** be via a guest login and not a Partnership login.

16 Equipment security and login credentials

16.1 The Partnership provides IT equipment solely for business purposes. Occasional personal use may be permitted as set out in paragraph 20 et seq. There is **no** provision for use by non-employees such as family members and friends.

16.2 Every school **must** have an asset register and ensure that all IT and communication systems equipment is logged on it. The central team will have its own register.

16.3 Individuals are responsible for the security of equipment allocated to or used by them, and **must not** allow it to be used by anyone other than in accordance with this policy.

16.4 As a minimum, individuals **must** lock their terminal or laptop, or log off, when leaving it unattended or on leaving the office, to prevent unauthorised users accessing the system in their absence.

16.5 Individuals not authorised to access the ICT network **must** only use desktop PCs, laptops or other devices under direct supervision.

16.6 Desktop PCs, cabling for telephones or computer equipment **must not** be moved or tampered with without first consulting the IT Technician, whether they be employed or a service provider. Significant changes such as the replacement or relocation of a server, server room or wireless provision **must not** be undertaken without first seeking the approval of the Head of Operations.

16.7 **Only** permitted staff may enter a server room or access a comms cabinet: for clarity, this will always be the Headteacher, IT Technician and Head of Operations, Site Manager and IT Service Provider.

16.8 Passwords or passphrases **must be** used on all equipment that allows access to the ICT network, including email and online storage, and when using Remote Desktop. The protocol for equipment and network access password or passphrases will be decided by the IT provider who will ensure that the latest industry best practice is followed.

16.9 New login credentials **must** be requested using the automated process which will ensure that relevant checks are carried out prior to approval, For example, that individuals are employees or governors or where they are not, that relevant disclaimers have been signed.

16.10 Equipment that is taken off site **must** be signed for using the **Loan of Equipment Agreement** at **Appendix A** and the appropriate asset register **must** be updated to reflect the item is in an individual's possession.

16.11 Equipment and network access passwords and passphrases **must** be kept confidential. Individuals **must not** use another person's credentials or make available or allow anyone else to log on using their own credentials. The only exception is to enable nominated ICT network providers and technicians to troubleshoot.

16.12 On the termination of employment or contract (for any reason) of any person described in 14.1.2, individuals **must** return any equipment, key fobs or security cards in their possession.

16.13 Individuals issued with a portable device such as a laptop, tablet computer, mobile phone or iPad, **must** ensure that it is kept secure at all times; items **must not** be left in vehicles unless absolutely necessary and special attention is required when travelling since documents may be read by third parties, for example, passengers on public transport. Individuals **must** be mindful of images stored on Partnership equipment which is taken off site and the Loan of Equipment Agreement **must** highlight this risk.

16.14 Equipment taken off Partnership premises **must not** be linked to unsecured public or private internet networks, such as public transport or café networks, or a mobile network that is not secured – a secure network will be indicated next to the network name.

16.15 It is strongly recommended that passwords or passphrases are used on all standalone IT equipment, such as iPads and smartphones, in order to ensure the security of locally stored data such as photographs of pupils. Exceptions are where to do so would be a barrier to teaching and learning.

16.16 It is expected that all desktops and laptops are network connected to ensure benefit from the protections outlined in 15.2 and regular system updates.

16.17 Individuals issued with a portable device are responsible for regularly connecting their equipment to the network and allowing time for system updates to be installed – this is particularly important for laptops.

16.18 Employees **must not** prevent updates running on any piece of Partnership equipment.

17 Systems and data security

17.1 Coastal Learning Partnership is the Data Controller. The Data Protection Policy describes how this duty is discharged.

17.2 Access to the ICT Network is given to employees in order for them to conduct Partnership business.

17.3 Individuals **must not** delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of their duties). This does not prevent individuals cleansing data storage to comply with the Partnership's Data Protection Policy and retention guidance.

17.4 Individuals **must not** download or install software from external sources without authorisation from the onsite IT Technician or IT service provider or Head of Operations. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files.

17.5 All software procured by the Partnership is subject to licensing agreements that comply with the statutory legal requirements and software licensing laws. Any software applications/programs privately procured and licensed to an individual are **not** to be loaded onto any Partnership equipment.

17.6 Data **must** be stored on network or cloud drives and folders, **not** on local drives or removable storage.

17.7 Individuals **must not** attach any device or equipment to the Partnership's ICT systems without prior authorisation. This includes any USB flash drive, MP3 player, tablet, smartphone or other similar device, whether connected via the USB port, infra-red connection or in any other way. Exceptions are keyboards, mice, speakers, headphones and IP telephony.

17.8 The use of memory sticks/USB flash drives/external hard drives, unless specifically authorised by the Partnership's Head of Operations, is **not** permitted. When an exception is requested, consideration will be given to the transportation of staff and pupil data, and the risk of loss or misuse of such data. If an exception is agreed, then an **encrypted memory stick** must be used and the ICT Provider must scan it before use.

17.9 Generic network profiles pose a risk to network and data security and their use is strongly discouraged. In the event that created decision is made to create a generic profile, a signed log will need to be retained to record the details of individuals given access and on what dates. This log will be used in the event of a breach or security incident.

17.10 Allowing community groups to access networked equipment creates a high risk and is not recommended. In this instance, it is vital that profiles are absolutely limited so that the user cannot see or access any school or Partnership documents.

17.11 Passwords or passphrases to all applications, databases and software used in the course of Partnership business **must** be kept private and not shared.

17.12 Individuals should exercise particular caution when opening unsolicited emails from unknown sources or an email which appears suspicious. The Partnership reserves the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.

17.13 Individuals **must not** attempt to gain access to restricted areas of the ICT network, or to any password or passphrase protected information, except as authorised in the proper performance of their duties.

17.14 Individuals using Partnership IT equipment off site **must** be vigilant and take precautions against importing viruses or compromising system security, remembering that our systems and IT equipment contain information which is confidential and/or subject to data protection legislation. Such information **must** be treated with extreme care and in accordance with our Data Protection Policy.

18 Email Security and login credentials

18.1 The Partnership provides email solely for business purposes. Occasional personal use may be permitted as set out in paragraph 20.

18.2 All Partnership email accounts **will** be protected by a password or passphrase protocol implemented by the IT provider who will ensure that the latest industry best practice is followed.

18.3 New login credentials **must** be requested using the automated process which will ensure that relevant checks are carried out prior to approval, For example, that individuals are employees or governors or where they are not, that relevant disclaimers have been signed.

18.4 All Partnership email accounts **must** contain the following footer disclaimer:

> *Coastal Learning Partnership may monitor the content of, and the email traffic data related to, both outgoing and incoming email communications. This monitoring is carried out on the basis of our legitimate interests and for the purposes of ensuring the security of our IT systems and training our staff. Data processed for these purposes will not be shared outside the Coastal Learning Partnership. Please refer to our privacy notices available on our website for more information about our data processing activities generally.*

18.5 Email messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

18.6 Partnership email accounts should not be used for personal business. Occasional personal use may be permitted as set out in paragraph 20 et seq.

18.7 Personal email accounts **must not** be used for Partnership business.

18.8 All business and school related email communication between staff and members of the school community **must** be made from a Partnership email account. In the event that a member of staff has a personal relationship with a member of the school community, they **must** ensure that professional and personal communications are kept separate and appropriate email addresses used for each. Advice should be sought from their Headteacher, Senior Leader or Head of Operations if uncertain.

18.9 Generic email accounts pose a risk to data security and are strongly discouraged especially for use by external supply. In the event that they are created, **Headteachers and Senior Leaders must** ensure a signed log is retained to record the details of individuals given access and on what dates. This log will be used in the event of a breach or security incident.

18.10 A distribution email or Teams or O365 group should be created for use by teams and groups such as school office and finance team. This can be done via the Partnership Intranet.

18.11 If email is used to share sensitive information with external partners and internally with colleagues on a different email domain, the email itself **must** be encrypted even if attached documents are password or passphrase protected. There is no need to encrypt emails that are sent internally on the same email domain.

18.12 In general, users **must not**:

18.12.1 Send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, or otherwise inappropriate emails.

18.12.2 Send or forward private emails at work which you would not want a third party to read.

18.12.3 Send or forward chain mail, junk mail, cartoons, jokes or gossip.

18.12.4 Sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals.

18.12.5 Agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter.

18.12.6 Download or email text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this.

18.12.7 Send messages from another person's email address (unless authorised) or under an assumed name.

18.12.8 Send confidential messages and personal/sensitive data via email which are not appropriately secure or encrypted; users will need to consider if they are sending an email on the same internal email domain and if the recipient is an external party.

18.13 If an individual receives an email in error, they should inform the sender immediately. It may also be necessary to inform the **Data Protection Officer** in the event that a cyber incident or breach has occurred.

18.14 Email best practice; users **must**:

18.14.1 Always consider if email is the appropriate method for a particular communication. Correspondence with third parties by email should be written professionally as a letter. Messages should be concise and directed only to relevant individuals.

18.14.2 Ensure a professional signature representing their school or the Partnership is used on all external emails. It is good practice to include the same signature on internal emails.

18.14.3 Aim to access emails at least once every working day and use an out of office response when away from the office for more than a day. Endeavour to respond to emails marked "high priority" within 24 hours.

18.14.4 Take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Remember, there is no control over where an email may be forwarded by the recipient. Avoid writing anything which would cause offence or embarrassment if it was forwarded to colleagues or third parties or found its way into the public domain.

18.14.5 Be alert to scam or phishing emails. Emails should be carefully checked for authenticity and links clicked on with caution. Suspicious emails should be reported to the Head of Operations, and in the event that a phishing link is clicked, the ICT provider and Head of Operations **must** be informed immediately so they may take steps to stop the spread.

18.14.6 Avoid contributing to system congestion by sending trivial messages, copying or forwarding emails to those who do not have a real need to receive them, or using "reply all" unnecessarily on an email with a large distribution list.

18.15 Users **must** immediately report to their line manager receipt of any email that makes them feel uncomfortable or is offensive, discriminatory, threatening or bullying in nature. Such communication **must** not be responded to until the user is instructed to do so; they may be instructed not to respond.

18.16 Pupils may be provided with individual or group school email addresses for educational use. In which case:

18.16.1 Their use **must** be compliant with the **Acceptable User Agreement** at **Appendix C**.

18.16.2 They will be taught how to report any communication which is inappropriate or makes them feel uncomfortable.

18.16.3 They will be taught to have an awareness of digital threats perpetrated by email.

19 Using the internet – general principles

19.1 The Partnership provides internet access solely for business purposes. Occasional personal use maybe permitted as set out in paragraph 20.

19.2 When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in paragraph 19.3, such a marker could be a source of embarrassment to the individual and the Partnership, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature.

19.3 Individuals **must** not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content which is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy. If such a site has been searched or accessed in error, this must be reported by the user to their line manager.

19.4 On occasion, content filtering may block access to a permitted internet site; users may contact the ICT Provider to have access enabled. Where the ICT Provider is concerned at this request, they must refer to the ICT Network Manager for clarification. If access to a site has been requested in error, this should be reported by the user to their line manager. It will appear on regular filtering reports and may be investigated.

19.5 Individuals **must** not under any circumstances use the ICT Network or Partnership equipment to participate in any non-work related internet chat room or message board or set up or log text or information on a blog or wiki, even in their own time. It is permitted to use work related chat rooms or message boards such as those utilised by platforms such as Arbor and learning platforms.

19.6 The following **must never** be accessed from the ICT Network: online audio and video streaming, instant messaging and personal webmail and social networking sites (such as Facebook, Twitter, Bebo, YouTube, Second Life) unless the access is for legitimate Partnership business. This list may be modified from time to time.

20 Personal use of the ICT network and our systems

20.1 We permit the incidental use of our internet, data storage and telephone systems to browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It **must** not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

20.2 Personal use **must** meet the following conditions:

20.2.1 Be minimal and take place substantially out of normal working hours.

20.2.2 Not interfere with work commitments.

20.2.3 Not commit the partnership to any marginal costs.

20.2.4 Does not adversely affect the performance of Partnership equipment.

20.2.5 Comply with this policy and other CLP policies including those listed at paragraph 14.2.

20.3 Individuals should be aware that personal use of our ICT Network may be monitored in accordance with our Privacy Notices and, where breaches of this policy are found, action may be taken under the disciplinary procedure (see paragraph 22). We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

21 Monitoring

21.1 Our systems enable us to monitor telephone, email, voicemail, internet and other communications. Use of our systems, including any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes including requirements set out in Keeping Children Safe in Education. Further information is available in the Partnership's Privacy Notices.

21.2 Where a CCTV system is used to monitor areas, this data is recorded. Further information is available in the Partnership's Privacy Notices and CCTV policy.

21.3 We may monitor the contents of email messages or check internet usage (including pages visited and searches made) as reasonably necessary and to the extent require by law, in the interests of the Partnership, including for the following purposes (this list is not exhaustive):

21.3.1 To monitor whether the use of the email system or the internet is legitimate and in accordance with this policy.

21.3.2 To find lost messages or to retrieve messages lost due to computer failure.

21.3.3 To assist in the investigation of alleged wrongdoing.

21.3.4 To comply with any legal obligation.

Further information is available in the Partnership's Privacy Notices.

22 Prohibited use of our systems

22.1 Misuse or excessive personal use of our ICT network, telephone or email systems or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some circumstances be a criminal offence.

22.2 In particular, it will usually amount to gross misconduct to misuse our systems by participating in online gambling, forwarding chain letters, or by creating, viewing, accessing, transmitting or downloading any of the following material (this list is not exhaustive):

22.2.1 Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature).

22.2.2 Offensive, obscene, or criminal material or material which is liable to cause public embarrassment to the Partnership.

22.2.3 The creation, possession, sharing or distribution of deepfake or image manipulated images – see paragraph 31.

22.2.4 A false and defamatory statement about any person or organisation.

22.2.5 Material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches any of our policies).

22.2.6 Confidential information about us or any of our staff or students/parents (except as authorised in the proper performance of your duties).

22.2.7 Any other statement which is likely to create any criminal or civil liability (for you or us).

22.2.8 Music or video files or other material in breach of copyright.

22.3 Staff **must not** use the ICT network or systems to support private commercial activity including 'hosting' web sites or conduct any form of non-Partnership business using Partnership equipment and resources

22.4 Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.

23 Use of Personal mobile, smart technology and cloud accounts – staff, Governors/Trustees, agency staff, volunteers and consultants (also known as Bring Your Own Device BYOD)

23.1 Any agreed use of personal mobile devices, smart technology and cloud accounts must not introduce vulnerabilities into existing secure environments.

23.2 Considerations about whether to use personal equipment for Partnership business will need to include: levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring (this list is not exhaustive).

23.3 **Senior Leaders** as defined in Section 4 should reduce the security and safeguarding risks posed by the use of personal mobiles by providing staff who rely on use of mobiles for their work with a Partnership mobile so they may use this exclusively for work. Examples include site managers.

23.4 **It is accepted that implementation of multi factor authentication requires the use of personal mobile devices in school in order to authenticate access to many applications; where possible school IP addresses will be whitelisted however it is acknowledged many applications do not enable this. Use of devices to authenticate access must be in line with paragraph 23.7.**

23.5 As a minimum, the following controls and limitations on the use of personal mobile devices, smart technology and cloud accounts for Partnership activities are required:

23.5.1 Individuals **must** adhere to our Data Protection and Safeguarding and Child Protection policies.

23.5.2 Personal devices will be covered by the Partnership's filtering systems while being used on the premises.

23.5.3 Audits and monitoring of usage may take place to ensure compliance.

23.5.4 The use of personal memory sticks/USB flash drives/external hard drives for storing Partnership data is **not** permitted.

23.5.5 Use of personal cloud accounts is **not** permitted, for example, the use of personal iCloud or Google Drive or One Drive to store and work on work documents – a work cloud account **must** be used at all times.

23.5.6 Personal devices **must not** be used to take images of children.

23.5.7 Personal accounts **must not** be used to discuss or share confidential Partnership business or discuss the personal information of staff or pupils and their families, either on or away from Partnership premises. For example, text messaging, using messaging applications such as What's App or Messenger, email accounts and email apps. Further clarification around the use What's App is provided in Appendix I.

23.5.8 Personal devices may only be used to discuss or share Partnership business or discuss pupils and their families if a Partnership account is being used, for example, via an email app on a mobile phone or iPad. Where possible, such an app should be used exclusively for Partnership business to ensure integrity.

23.5.9 Creating and editing documents containing Partnership data, particularly personal data, using personal equipment is **only** permitted via use of Remote Desktop or using Partnership cloud based accounts, such as OneDrive.

23.5.10 Personal mobile phones **must not** be used to make contact with parents and carers on school business, nor should any such contact be accepted.

23.5.11 Mobile phones and other mobile devices **must not** be left unattended in any areas where there are children due to the risk posed by the ability to take images and immediately post them online.

23.5.12 Senior Leaders as defined in Section 4 **must** ensure expectations of visitors on the use of personal devices are clear at point of signing in to ensure visitors to Partnership sites are able to comply.

23.6 As a minimum, the following arrangements must be in place if using personal devices such as a laptop for professional use at home or in school:

23.6.1 Devices **must** be password or passphrase protected and default passwords or passphrases not used.

23.6.2 Remote desktop or browser applications **must** be used to access school documents, folders and the internet in order to minimise the risk of inadvertently sharing personal data, and these must have multi factor authentication protection. In the event that remote desktop or cloud browser applications are not available, staff **must** seek approval from a senior leader and ensure that:

(a) All personal applications and documents are closed so they cannot be inadvertently accessed or copied.

(b) Pop ups are disabled and notifications turned off.

23.6.3 Devices **must** have up to date anti-virus software is installed.

23.6.4 The device and applications are kept up to date. The National Cyber Security Centre explains that, *Applying software updates is one of the most important things you can do to protect yourself online. Update all the apps (and your device's operating system) whenever you're prompted. It will add new features and immediately improve your security*.

23.6.5 No documents are stored locally on the device or on removable storage.

23.7 It is accepted that most staff are extremely likely to have a personal mobile device in school and its use as described in this policy has been informed by DfE guidance, Mobile phones in schools[12].

[12] https://www.gov.uk/government/publications/mobile-phones-in-schools/mobile-phones-in-schools

23.8 A mobile phone is necessary to authenticate access to many applications as per paragraph 23.4. Although permitted, staff **must** accept responsibility for their device and **must** adhere to the expectations and limitations set out in this policy and **must** adhere to school arrangements. This requirement is reflected in the Staff Code of Conduct. For example:

23.8.1 Staff must use their personal device away from pupils.

23.8.2 Staff must use their personal device while on a designated break or during non-contact time.

23.8.3 It is accepted that some non-teaching staff, for example, site managers and central team staff, require a greater freedom to use devices whilst at work. They will ensure that their use is minimal, does not impact colleagues and their work and is away from pupils.

23.8.4 Personal phone calls should only be made or taken whilst on a designated break and away from pupils. If a member of staff has a situation outside of school which they feel may require them to have ready and immediate access to their personal device, they should discuss with their Headteacher or Senior Leader.

24 Use of Personal mobile and smart technology – pupils (also known as Bring Your Own Device BYOD)

24.1 The Partnership recognises that many children have access to personal communication devices including mobile phones, smart phones and smart watches. Pupils' use of such technology as described in this policy has been informed by DfE guidance, Mobile phones in schools.

24.2 The use of personal technology by pupils whilst at school is **not** permitted. Use of such devices at school is a distraction from learning and introduces safeguarding risks and cyber vulnerabilities.

24.3 Senior Leaders, Designated Safeguarding Leads and Online Safety Champions are required by this policy to be mindful of the learning distractions and safeguarding vulnerabilities introduced by such technology and to ensure these are reflected in behaviour policies.

24.4 CLP discourages its families from allowing children to bring a device, such as a mobile phone, to school. It is recognised that some families consider that their child requires access to a phone for the journey to / from school. If a child is permitted by their parents to bring such a device to school, it **must** be:

- Switched off on arrival into the school grounds.
- Handed in to an adult according to the school's particular arrangements.
- Collected at the end of the school day.
- Turned on only once the pupil has left the school grounds except in emergencies or if specifically permitted by a school employee.

24.5 Exceptions may be granted by the Headteacher where reasonable adjustments are considered appropriate, such as a child requiring a mobile phone to manage /track a medical condition. Government guidance on mobile phone restrictions specifically recognises that some pupils need access to a phone for medical reasons such as diabetes.

24.6 Even when such exceptions are authorised by the Headteacher, any use of such a device **must** be in line with the **Acceptable Use Agreement** at **Appendix C**.

24.7 Devices brought into school and used inappropriately and/or not handed in for safekeeping as required by this policy will be confiscated. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school's behaviour policy.

24.8 Pupils should not bring a tracking device to school, or on any educational visit. Whilst at school, school staff are responsible for maintaining effective supervision of the pupils. Tracking devices (e.g. AirTags, GPS trackers, GPS-enabled smartwatches) raise safeguarding, privacy and operational concerns and are considered inappropriate because:

- Such devices can reveal the location of not only an individual, but a whole group which can be problematic where children are subject to safeguarding plans and protection orders.
- Disclosing the location of others who have not consented is not appropriate.
- Location data can be inaccurate or disabled and can lead to unnecessary parental anxiety if a device appears to be in an unexpected location or loses connectivity.
- It risks undermining the role of staff as supervising adults and undermining parental trust in the adults looking after their children.

24.9 Pupils must therefore not bring or wear AirTags, GPS trackers or other personal location-tracking devices during the school day or on educational visits unless expressly authorised by the Headteacher in exceptional circumstances.

24.10 School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. The DfE provides guidance to schools on searching, screening and confiscation[13].

24.11 When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff **must** reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm; and/or
- Disrupt teaching; and/or
- Break any of the school rules.

24.12 If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material; or
- Retain it as evidence; and/or
- Report it to the police.

24.13 Any searching of pupils will be carried out in line with government guidance[14][15]:

24.14 In all cases where any such action has been taken, schools will liaise closely with parents/carers.

24.15 Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

---

[13] https://www.gov.uk/government/publications/searching-screening-and-confiscation
[14] https://www.gov.uk/government/publications/searching-screening-and-confiscation
[15] https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

25 Acceptable Use Agreements (AUAs) and issues of misuse

25.1 Agreements can be found at **Appendix C:**

25.1.1 Staff **must** sign the AUA annually – this will usually be done digitally via a centrally chosen platform. A shorter version will be displayed on login which staff must agree to before logging in.

25.1.2 The pupil AUA must be displayed in the area(s) where pupils use computers and on login which pupils must agree to before logging in.

25.1.3 The parent AUA will be displayed on every school's website and will be referenced in the Parent Code of Conduct. Schools will include a link to the school website location in their newsletters.

25.1.4 On first admission, the pupil and parent AUA will form part of the digital admissions onboarding so that digitally acknowledgement is received and can be uploaded to the pupil MIS system.

25.1.5 Governors and Trustees **must** sign the AUA annually – this will usually be done digitally via a centrally chosen platform.

25.1.6 All staff, including casual staff, must sign the AUA.

25.1.7 An external individual allocated an account, likely to be SCITT or Agency Supply or nominated consultants, must sign the disclaimer at **Appendix H** and the staff AUA.

25.2 Misuse of IT and communications systems can cause financial and reputational damage to the Partnership.

25.3 The Acceptable Use Agreement is intended to ensure that:

25.3.1 Staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational and professional and personal use.

25.3.2 Children will be responsible users and stay safe while using the internet and ICT tools

25.3.3 The CLP network and systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

25.3.4 Staff are protected from potential risk in their use of technology in their everyday work.

25.3.5 Parents/carers are aware of the importance of online safety and are involved in the education and guidance of children with regard to their on-line behaviour.

25.3.6 Parents are mindful of the impact of their own use of technology on the school community.

25.4 Where a pupil misuses the ICT network or school's systems or the internet, or breaks the Acceptable Use Agreement in any way:

25.4.1 Schools will follow the procedures set out in their behaviour policy and/or any other appropriate policy.

25.4.2 Action taken will depend on the individual circumstances, nature and serious of the specific incident, and will be proportionate.

25.4.3 School leaders may consider it necessary to inform the Head of Operations of the incident should technical or system improvements or changes need to be considered or supporting evidence be required.

25.5 Where a staff member misuses the ICT Network, systems or the internet, misuses a personal device, or breaks the Acceptable Use Agreement in any way:

25.5.1 The action will be considered as a breach of this policy and will be dealt with in accordance with our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

25.5.2 Managers dealing with any part of this policy **must** ensure that HR are informed of the details and given copies of relevant documents.

25.5.3 Action taken will depend on the individual circumstances, nature and serious of the specific incident, and will be proportionate.

25.5.4 Managers and/or the HR Team may consider it necessary to inform the Head of Operations of the incident should technical or system improvements or changes need to be considered or supporting evidence be required.

25.6 Where Governors/Trustees, agency staff, volunteers or consultants working in schools misuse the ICT Network, the responsible Senior Leader as defined in Section 4 should be made immediately aware who will in turn inform the Head of Operations. Together they will decide on the most relevant action / outcome.

25.7 If any incident of misuse is potentially illegal or serious in nature, a report should be made to the police.

26 Equipment Loaned to Pupils

26.1 Schools may make provision to loan equipment to pupils. This equipment may have been procured by the school or through a scheme, for example, through the Local Authority or the DfE.

26.2 Schools **must** ensure that all devices are installed with a suitable licence for software for safeguarding (filtering and antivirus) purposes.

26.3 Schools should adopt the letter at **Appendix B** when equipment is loaned to pupils.

27 New Technologies

27.1 The aim of this policy is not to stifle innovation but to ensure that all our pupils, staff and partners are able to use technologies with confidence, safely and without compromising either themselves or Coastal Learning Partnership.

27.2 For this reason, it is essential that due regard is given to the introduction of new technologies and that processes designed to safeguard all are followed.

27.3 When considering the use of a new technology, the **CLP Data Protection Policy** and the General Data Protection Regulation (GDPR) require a **Data Protection Impact Assessment (DPIA)**.

28 Online Safety

28.1 The internet and online technology provide new opportunities for pupil's learning and development, but it can also expose them to risks, particularly risks that may not be obvious to them. Children and young people need help and support to recognise and avoid online risks and build their resilience.

28.2 Keeping Children Safe in Education emphasises the importance of the education of pupils and staff in online safety and categorises four areas of risk: content, contact, conduct and commerce

28.3 Online safety therefore should be a focus in all areas of the curriculum.

28.4 To help prevent cyber-bullying, schools will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. They will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

28.5 School DLSs must ensure that procedures are in place for handling attempted access to harmful content.

28.6 Schools will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Cyber bullying will be addressed at high-profile opportunities such as assemblies and by engaging with national events such as 'Safer Internet Day'.

28.7 The curriculum in schools includes opportunities to teach children about issues related to cyber-bullying. This is an element of the computing curriculum but also features within areas such as personal, social, health and economic (PHSE) education. Schools will work with other partners such as the local police safe schools/community teams to facilitate regular opportunities for pupils to leaning about issues relating to online safety.

29 Education – parents / carers

29.1 Parents and carers play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours, but they may only have a limited understanding of online safety risks and issues.

29.2 Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

29.3 Schools will educate parents / carers in online safety and this will include educating about cyber-bullying: what it is, how it can be identified and reported, how it can be prevented and how it can be stopped.

29.4 Online Safety Champions will work with school leaders to deliver training and information as set out in Section 6.

29.5 School staff will encourage parents and carers to support good online safety practice and to follow guidelines on the appropriate use of:

29.5.1 Digital and video images taken at school events.

29.5.2 Access to parents' sections of the website / blog.

30 Education & Training – Teaching Staff, Volunteers and Governors

30.1 It is essential that all teaching staff receive regular, and at least annually, online safety training and understand their responsibilities, as outlined in this policy.

30.2 Online Safety Champions will work with school leaders to deliver training and updates as set out in Section 6.

31 Digital Images

31.1 Staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place.

31.2 Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

31.3 Where nude and semi-nude images are found to have been shared, members of staff **must** refer to the guidance issued by the Department of Science, Innovation and Technology Sharing nudes and semi-nudes: how to respond to an incident (overview) (updated March 2024). This guidance clearly states incidents must be reported to the Designated Safeguarding Lead (DSL) or equivalent immediately, and advices:

- **Do not** delete the imagery or ask the young person to delete it.

- **Do not** ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).
- **Do no**t share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain to them that you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

31.4 The following is prohibited: the creation, possession, sharing or distribution of AI-generated content that:

31.4.1 Depicts a member of the school community without consent.

31.4.2 Creates false sexual imagery.

31.4.3 Creates false criminal or abusive behaviour.

31.4.4 Damages an individual's reputation.

31.4.5 Attempts to deceive staff, parents or pupils.

31.4.6 All deepfake incidents will be referred immediately to the Designated Safeguarding Lead.

32 Taking and use of images

32.1 Staff may take digital / video images of pupils and colleagues to support educational aims, but **must** follow this policy and the **CLP Data Protection Policy** concerning the sharing, distribution and publication of those images.

32.2 Such images **must only** be taken on school equipment.

32.3 Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school, and therefore the Partnership, into disrepute.

32.4 Schools should:

32.4.1 Encourage children to tell them if they are worried about any photographs that are taken of them.

32.4.2 Carefully consider involving very young or vulnerable children when taking photos or recordings, as they may be unable to question why or how activities are taking place.

32.4.3 Discuss the use of images with children and young people in an age-appropriate way.

32.5 Images will not be taken of any child or young person against their wishes. A child or young person's right not to be photographed is to be respected, and this right should not be confused with the General Data Protection Regulation (GDPR).

32.6 Photography is not permitted in sensitive areas such as changing rooms, toilets, swimming areas, areas where children may be intimately changed, etc. Exceptions are for reasons of premises management and these areas **must** be empty of children before a photograph is taken.

32.7 Photographing of a sleeping child or a child engaged in toileting activities is not permitted; these activities can be recorded for parents with words.

32.8 The use of digital images on websites, educational software or in other publications such as newsletters **must** comply with this policy and the **CLP Data Protection Policy**.

32.9 Schools should not attempt to enforce unreasonable or unwieldy restrictions. It is very likely that during a public event such as a school performance or school disco or school fayre where parents and carers are present that they will want to take photographs and it **must** be accepted that these photographs are likely to be shared with family members and on social media. Rather than try to introduce restrictions which the school cannot police, schools should instead educate parents about sharing safely and perhaps provide managed opportunities for photographs, such as at the end of a performance. Schools should not provide a reassurance that photographs will not be taken by other parents, but should instead manage expectations and work with parents who are concerned about photographs.

33 Social Media and Private Messaging Applications / Software

33.1 The widespread availability and use of social media applications bring opportunities to understand, engage, and communicate in new and exciting ways and Partnership staff **must** be able to use these technologies and services effectively and flexibly. It is, however, critical to ensure we balance the use of technologies with our duties to our pupils and schools, our communities, our legal responsibilities and our reputation.

33.2 In particular, use of social networking and private messaging applications has implications for our duty to safeguard children, young people and vulnerable adults.

33.3 This section provides staff with a framework of good practice and ensures that any users are able clearly to distinguish where information provided via social media is legitimately representative of the Partnership or the schools.

33.4 It applies to all Coastal Learning Partnership staff, regardless of job role, and users of the network, including consultants, agency staff and service providers.

34 Use of Social Media and Private Messaging Applications in practice

34.1 Social networking applications include, but are not limited to:

34.1.1 Blogs, online discussion forums, collaborative spaces, media sharing services, and online gaming environments. Examples include Twitter, Facebook, Windows Live Messenger, YouTube, Flickr, Xbox Live, Tumblr, LinkedIn and comment streams on public websites such as newspaper sites.

34.1.2 Many classroom learning environments provide social media opportunities. Examples include Class Dojo, Google Classroom, and Seesaw. [Note: the use of Class Dojo for anything other than general communications with parents, those that are not child specific, is not encouraged due to the always available nature of the platform and because of breaches that have occurred.]

34.2 All members of staff should bear in mind that information they share through social networking and private messaging applications, even if they are on private spaces, are still subject to copyright, Data Protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They **must** also operate in line with the Partnership's Equalities, Safeguarding and Child Protection, Data Protection and this policy.

34.3 Within this policy there is a distinction between approved use of social media for professional business and educational purposes, and personal use of social media.

35 Personal Use of Social Media and Private Messaging Applications

35.1 All staff should exercise caution before inviting, accepting or engaging in personal social media communications with parents or children from Partnership school communities whilst employed by Coastal Learning Partnership.

35.2 It is accepted that social media relationships may have been established prior to employment and that family relationship may exist. In such cases, it is advisable for staff to:

35.2.1 Inform their Senior Leader as defined in Section 4 of the relationship.

35.2.2 Refrain from responding to any comments made by contacts on social media about Partnership business.

35.2.3 Inform their Senior Leader as defined in Section 4 if they feel compromised by any social media relationship.

35.3 Any communication received from children on any personal social media sites **must** be reported to a Designated Safeguarding Lead in the relevant school.

35.4 All staff who become aware of any inappropriate communications involving any child in any social media, **must** immediately report to a Designated Safeguarding Lead, even if the child is not from a Partnership school.

35.5 All staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.

35.6 Personal social media accounts **must not** be used to publish photographs of pupils or school activities.

35.7 All staff are advised to avoid responding to posts or comments that refer to specific, individual matters related to the Partnership and members of its community on any social media accounts.

35.8 All staff are expected to consider the reputation of the school in any posts or comments related to the Partnership on any social media accounts.

35.9 All staff **must not** accept any current pupil of any age or any ex-pupil of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account.

35.10 Staff **must** not access personal social media accounts on school grounds unless on an agreed break and away from areas where there are pupils.

35.11 Personal social media accounts **must not** be accessed on Partnership / school equipment.

35.12 Staff **must not** name their specific place of work or employer on any social media account; the exception being LinkedIn.

36 Approved business and professional use of social media

36.1 There are many legitimate uses of social media within the curriculum and to support student learning. For example, class blogs, school Facebook pages, classroom learning environments and platforms, and academy Twitter accounts. When using social media for educational purposes, the following practices must be observed:

36.1.1 A distinct and dedicated social media site or account for educational purposes **must be** created. This should be entirely separate from any personal social media accounts held by member of staff, and should be linked to an official Partnership email account.

36.1.2 The URL and identity of the approved site should be notified to the Headteacher before access is permitted for students and the Headteacher **must** ensure a log of all social media accounts is maintained by the school.

36.1.3 The content of any approved Partnership social media site should be solely professional and should reflect well on the Partnership and the school.

36.1.4 Staff **must** not use or publish photographs of children without ensuring the appropriate consents have been gathered; the **Data Protection Policy** refers.

36.1.5 Care **must** be taken that any links to external sites from the account are appropriate and safe.

36.1.6 Any inappropriate comments on or abuse of approved Partnership social media accounts should immediately be removed and reported to a Senior Leader as defined in Section 4.

36.1.7 Staff should not engage with any direct messaging of parents or pupils through social media where the message is not public.

36.1.8 Staff **must** consider carefully their use of private messaging applications with parents; staff are **strongly advised** to conduct all conversations regarding pupil attainment, behaviour and welfare are conducted using email, face to face or the school's MIS communication application.

36.1.9 All social media accounts created for educational purposes should include a link in the *About* or *Info* page to this policy via the Partnership website.

37 Pupils' use of social media

37.1 Pupils are taught about the risks associated with internet usage and to conduct themselves sensibly and safely on social media platforms. Under the General Data Protection Regulation 2018, parental consent is required to process the data of children under the age of 13 online where the processing, in an information services context, is reliant on consent. Pupils will be encouraged to adhere to this requirement, as it is designed to protect them online from illegal data collection and processing.

37.2 CLP schools will not tolerate:

37.2.1 Cyber bullying and persecution of individuals through abuse and harassment.

37.2.2 The posting of inappropriate content, including the overtly sexual, or racist, sexist or homophobic opinions.

37.2.3 The distribution of non-consensual or sexual images.

37.2.4 The abuse of staff, school, or aggressive criticism of site practices.

37.3 Incidents will be dealt with in accordance with relevant policies and in equal weight to acts of harassment, bullying, abuse or hate speech perpetrated on site.

37.4 Pupils are encouraged to report concerns and are aware of the channels of support available.

38 Video Conferencing and Live Stream Remote Working

38.1 Remote working has become common practice and both teaching and non-teaching staff increasingly work from home. Video conferencing enables flexible working and allows staff to attend meetings and connect with governors/Trustees, colleagues, contractors and consultants, service providers and our families. Video conferencing also enables governors and Trustees to conduct their business remotely.

38.2 Many schools provide a digital education platform to enable remote learning. Whilst the expectation is not for live stream lessons, the technology is there for schools to make use of to enhance their teaching and learning provision and to ensure lessons are available to pupils who may not be able to attend school. Keeping Children Safe in Education provides and signposts guidance for the safe delivery of remote education.

38.3 Video conferencing and live stream opens up the workspace to external elements and all users need to understand the potential security and safeguarding compromise this presents to the Partnership and be vigilant to the risks and understand how best to minimise them.

38.4 Coastal Learning Partnership has chosen to make MS Teams its video conference facility of choice for business purposes; it is included in the existing business software provision and integration into existing audit and monitoring capabilities are consequently in place.

38.5 The framework of good practice at **Appendix E** applies to all users who might need to make use of video conferencing or live stream facilities professionally, including consultants, agency staff and service providers acting on behalf of and conducting Coastal Learning Partnership business.

38.6 All users should bear in mind that information they share through video conferencing and live stream applications, even if they are on private spaces or personal equipment, are still subject to copyright, Data Protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.

38.7 Staff and governors/trustees, including contractors, consultants and service providers acting on behalf of Coastal Learning Partnership **must** not use a private video conferencing or live stream account to host a professional meeting or conference; only accounts registered with the Partnership **must** be used.

38.8 If using video conferencing or delivering livestream lessons or assemblies on a personal device such as a laptop, staff **must** follow the guidance set out in Section 23 of this policy.

38.9 Examples of other video conferencing applications which our business partners might use include, but are not limited to:

38.9.1 Zoom, Join Me, Google Hang-outs, Cisco Web-Ex.

39 Approved use of video conferencing for professional and business use

39.1 At all times users **must** be aware of confidentiality and security.

39.2 Users **must** be aware that video conferencing services often include extra features such as:

39.2.1 File sharing

39.2.2 Screen sharing

39.2.3 Instant messenger chat

39.2.4 Automatic call transcript generation

39.2.5 Remote control of another participant's device

It is recommended that these features are only utilised when on MS Teams via a Partnership account to ensure integrity.

39.3 Users should be aware that many services allow calls to be recorded, and for text chats and shared files to be saved:

39.3.1 When using an MS Teams Partnership account, storage is on the ICT network.

39.3.2 When using a non- Partnership account, storage is on the host's network.

39.4 At all times, users should be aware of the platform they are using.

39.5 A **best practice guide for Video Conferencing** can be found at **Appendix E**.

40 Live Stream Remote Learning

40.1 Remote Learning enables the Partnership to deliver home learning to pupils when it may not be possible for teachers and pupils to be together in a classroom. The partnership will consider remote learning provision as part of any disaster recovery response to a business continuity incident.

40.2 It is important to acknowledge that parents and families have a right to opt their children out of livestream learning. Schools should ensure there is an alternative remote learning plan in place for pupils in this position.

40.3 Schools **must** consider a pupil's access to the necessary IT hardware and the support they have at home when considering delivery of and engagement with remote learning. Schools will make every possible effort to ensure that they overcome any barriers which may prevent individual pupils from being able to fully engage with an online learning offer.

40.4 The superuser for each school:

40.4.1 **Must** be someone who has the technical knowledge and ability to administer the account and access controls.

40.4.2 Will be responsible for access control and management to ensure each user has the right level access for their role and that all class participants are correct.

40.4.3 **Must** ensure they only whitelist domains that are trusted; it may sometimes be necessary to allow external users access, for example, colleagues on a different domain.

40.5 Staff **must** ensure that communications with pupils and parents are professional and adhere to the Acceptable User Agreement requirements.

40.6 Staff, parents and pupils **must** adhere to the **Pupil and Parent Code of Conduct for Livestream Learning** at **Appendix D**. Parents and pupils **must** be required to read and sign this code of conduct before the pupil can participate in any live online learning. Just as they would regularly revisit behaviour expectations in a normal classroom environment, so staff should take opportunities to remind pupils of the expectations within this code of conduct.

40.7 Staff **must** ensure that communications from pupils and parents adhere to the Acceptable User Agreement requirements and where they fall short, they **must** ensure this is addressed and the Headteacher informed.

40.8 Schools **must** give due regard to the privacy and safety of themselves and all pupils and especially those pupils who are:

40.8.1 Looked After (LAC)

40.8.2 Subject to Child Protection plans

40.8.3 Pupils in sensitive situations such as parent separation

41 Generative artificial intelligence (AI) in education

41.1 The use of generative AI in education is developing and supported by the government[16].

41.2 Although the partnership encourages staff to make use of generative AI, it is paramount that staff are alert to the vulnerabilities that use of new technology brings and that they follow the expectations and parameters set out in the Trust's **AI and Data Protection Policies**.

41.3 Keeping Children Safe in Education 2026 introduces explicit guidance specifically regarding generative AI, AI-generated images, deepfakes, "Nudification" and image-manipulation tools, AI-related online harms to pupils and requires any AI product proposed for use with pupils to undergo a safeguarding impact assessment and review by the DSL, Data Protection Officer and IT service provider prior to implementation; all staff are responsible for reading and understanding the **AI Policy** before using any AI technology.

41.4 The Acceptable Use Agreement reflects these requirements.

[16] Generative artificial intelligence (AI) in education - GOV.UK

Appendix A: Loan of Equipment Agreement

(It is intended that this form will be digitalised in autumn 2026.)

The loan of equipment and remote access to the ICT network is given to employees and other named individuals to enable them to conduct their business away from their school or office base and is given as a privilege and not a right. All individuals to whom equipment is loaned, must use it responsibly and strictly in accordance with this policy and the following conditions:

- Loaned equipment remains the property of Coastal Learning Partnership.
- Equipment can only be removed from Partnership premises when the relevant asset management record is annotated and this agreement is signed. Both prior to removal.
- Use of equipment is permitted only by the person to whom it is issued; equipment is not to be loaned to any friend, or family member, or any other person.
- Partnership equipment is for professional use only. It is accepted that incidental personal usage is reasonable, however, equipment **must not** be used as a personal storage device, including for photographs and music.
- Staff and external individuals may be liable for the cost of replacement devices due to loss or damage due to misuse whilst in their possession, particularly staff allocated a device.
- Provisions in this policy and all policies named in paragraph 14.2 of this policy must be adhered to.

1. ITEMS TO BE BORROWED

Full description of equipment:	**Serial numbers:**	**Asset tag number:**

2. BORROWER

Name:	**Position:**	**Date:**

3. DECLARATION

I have read and will adhere to this policy agree to the safekeeping of the equipment detailed above and to the conditions detailed above. I understand that:

- Equipment **must not** be left unattended in a vehicle unless absolutely unavoidable.
- Loss of or theft of electrical, audio or visual equipment in my possession may not covered by the RPA (insurance) and I may be liable for replacement costs (which I may be able to claim from my personal insurance).

- All breakages, faults or losses must be reported immediately to the Headteacher or Senior Central Leader to whom I report.
- Loss or damage to the equipment may result in an investigation and consideration under the Partnership's HR policies and I may be liable for replacement costs.
- I must return equipment when asked to, and if borrowing Trust equipment for one year or longer, I am required to return the equipment for checking at the end of each twelve-month period.
- I am responsible for the secure storage of data, including sensitive data, on this device, and that I must be especially mindful of using equipment in public where images and other documents stored on Partnership might be seen by the public.
- I must not connect the device to an unsecured public network such as at railway stations or cafes. When connecting to any network it must be an encrypted password or passphrase protected network such as WPA2.
- I will not allow Partnership / school equipment in my possession to be used by non-employees such as family members or friends.

Signed: _____

APPROVAL

Name:	**Position:**	**Date:**

Signed: _____

4. RETURN OF ITEM

I confirm that the above item(s) have been returned in a satisfactory condition:

Name:	**Position:**	**Date:**

Signed: _____

Appendix B: Loan of Equipment to Pupils letter template

Dear Parent or Carer,

TERMS AND CONDITIONS REGARDING THE LOAN OF A LAPTOP OR TABLET COMPUTER

The laptop or tablet computer issued to your child or foster child with this letter of terms and conditions is intended for educational purposes. It is issued on a loan basis for six years from the date of issue and remains the property of [insert school name or council name or DfE or other as appropriate].

Regular supervision must be in place whilst your child is using the device to ensure that s/he is using it safely and not misusing it. In particular, you must consider how you monitor Internet and social media usage. Special care must be taken if your child wishes to install additional software or applications on it. Email and downloading from the Internet are prime sources of viruses and other malicious software. Unacceptable use of the device includes using, transmitting or seeking pornographic, offensive, obscene, criminal, vulgar, abusive, harassing, threatening, racist, sexist, discriminatory or defamatory language or materials.

You are expected to provide adequate desk and storage space for the device. It is strongly recommended that it is situated in a communal room rather than your child's bedroom.

If the device is damaged, lost or stolen, there will be a charge for the cost of repair or a replacement. The school is unable to provide technical support for the device beyond ensuring it has suitable safeguarding software installed.

If your child moves to live with another parent or carer, the device must move with your child. Please notify your child's school if this happens so that a new copy of these terms and conditions can be issued to the other parent or carer. If for any reason the device is no longer required, it should be returned as soon as possible to your child's school.

If your child moves school, the device will move with them and the new school will be told your child has been issued with a device. You should then contact them for any queries.

Please indicate your acceptance of these terms by signing and completing both copies of this letter in the form below. Please retain one copy for your records and return the other copy to your child's school.

Yours faithfully,

Coastal Learning Partnership

Name of child: _____

By signing this form, I agree to the above terms and understand that if the device is damaged, lost or stolen, there will be a charge towards the cost of repair or replacement.

Signature: _____

My name printed: _____

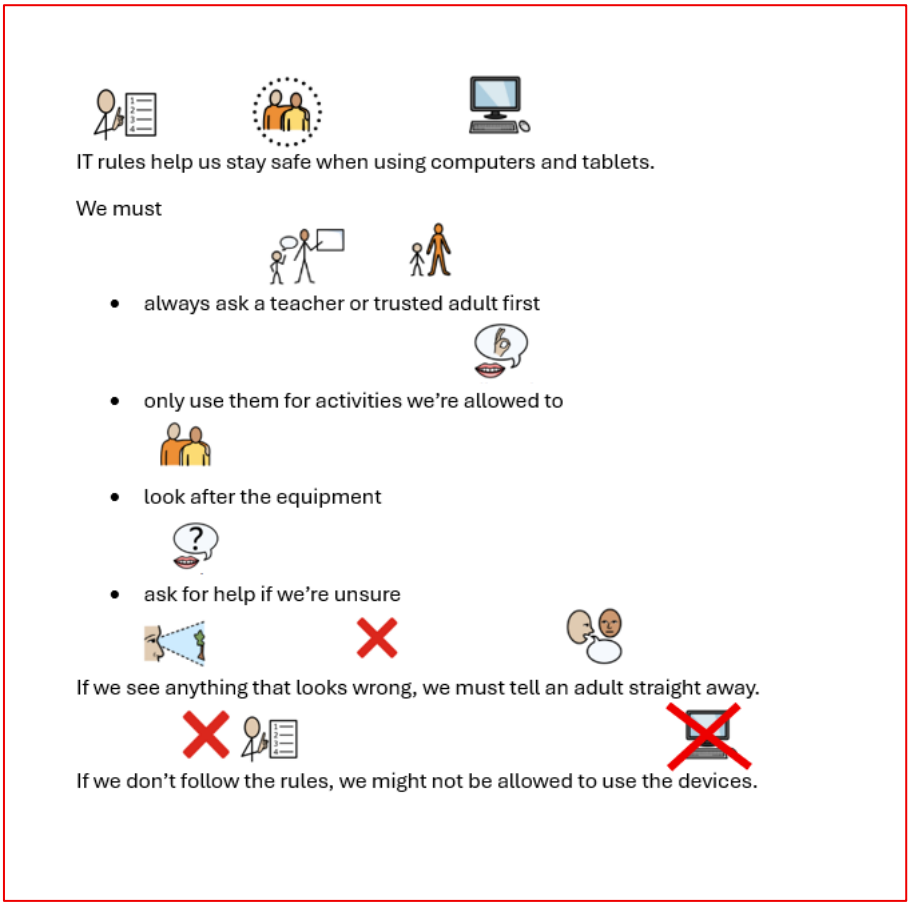
Relationship to child (e.g., mother/father/registered carer):

Address:

Date:

Appendix C: Acceptable Use Agreements

Acceptable Use Agreement – EYFS / KS1 pupils



Acceptable Use Agreement – KS2 pupils

Acceptable use of the ICT Network, school systems and internet: ***Agreement for Pupils***
Name of pupil:

I understand that I must and will:

- Always take care of all school equipment (including computers, cameras and headphones).
- Only use school technology for school-related work and with permission from a suitable adult.
- Only use systems and products that have been approved for my use.
- Not knowingly access any inappropriate websites or start any inappropriate online searches.
- Not go on any social networking sites at school (unless an adult has allowed this as part of a learning activity).
- Not use chat rooms whilst I am school.
- Not open any attachments in emails, or follow any links in emails, without first checking with a teacher.
- Not upload or download to and from the school network (including using USB devices).
- Not use any inappropriate or unkind language when communicating online, including in emails.
- Keep my login credentials (e.g., username and password or passphrase) to access the school network safe and secure; I will not try to log in to the school's network using someone else's details or try to access any other person's account or documents.
- When researching online, do my best to check that information is truthful and accurate and avoid plagiarism (copying).
- Immediately tell an adult if I see any unpleasant or inappropriate materials, or anything which makes me feel uncomfortable.
- Be polite and respectful and not take part in cyber-bullying and report any that I know about as soon as possible.
- Be aware of 'stranger danger' when communicating online and will not share any of my personal information (including my name, address, telephone number, date of birth)
- Take part in online learning responsibly and follow the rules my teacher sets me.
- Use technology safely and showing respect towards others both in and out of school.

I understand that the school will monitor the websites I visit.

If I bring a personal mobile or smart technology device such as a mobile phone or smart watch into school:

- I will turn it off as soon as I enter the school grounds and hand it in to be kept safe for the day.
- I will not switch it on again until I leave the school grounds except in an emergency.
- I understand that the school can confiscate such an item that I do not hand in.
- I understand that the school can search for and delete images or files that are inappropriate in line with *Searching, screening and confiscation* guidance.

Exceptions:

- I understand that exceptions may be approved by the Headteacher. If I am given permission to use my personal device, I understand this would be a privilege and because of a specific reason and that I must only use it for this reason, for example:
    - Medical reasons
    - Learning reasons
- I understand if I abuse this privilege that my use of my devise will be withdrawn.
  I understand that I must look after my own equipment and that my family and I are responsible for it and that the school is not under any obligation to pay for repair or replacement.

Acceptable Use Agreement for staff, Governors/Trustees, agency staff, volunteers or consultants working in schools

Acceptable use of the ICT Network, school systems and internet:
Agreement for staff, Governors/Trustees, agency staff, volunteers or consultants working in schools or remotely for CLP

Declaration:

- I understand that I must use the CLP network and systems and equipment in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.
- For my professional and personal safety, I will read and understand this **IT and Communications Systems Policy**, the **Data Protection Policy** and the **AI Policy** and abide with the provisions within them.
- I understand that I must read carefully, understand and adhere to Part Two of this policy, and where I do not understand what is required that I must seek an explanation or further guidance from a colleague such as:
    - My Headteacher
    - HR
    - Online Safety Champion
    - Designated Safeguarding Lead
    - The Head of Operations who is also the IT Network Manager
- I have read and understood paragraph 25 et seq with regards to misconduct and discipline.
- I understand that multi factor authentication (MFA) is enforced across our M365 and Google network and that I must set up the authentication app in order to access emails, documents and folders, Teams and other features.
- I understand that personal devices connected to CLP internet will be monitored by CLP filtering arrangements and that searches that cause concern may trigger an investigation.
- I understand that I must not store any work-related documents (unless specific to my employment) on any of my personal devices.
- I understand that I must not store any work-related documents / items to a personal cloud account, including iCloud and Google Drive. I understand I must use only a work cloud account for work purposes.
- My What's App will comply with Appendix I.
- I will not use any other messaging apps to communicate about work matters.
- I understand my use of AI must comply with the AI Policy. Specifically:
    - I will not use a system or product that is not listed on the approved register on the CLP Intranet.
    - If I identify a new AI system or product, I will ensure that the approval process is followed **before** using it – namely the Data Protection Impact Assessment (DPIA) process.
- If I become aware that AI is being used for the following, I will report immediately to a Designated Safeguarding Lead (DSL):
    - Bully another pupil.
    - Create sexualised content.
    - Impersonate an individual.
    - Groom or exploit children.
    - Distribute misleading or harmful content.
- I will ensure that I complete and sign the **Loan of Equipment Agreement** before taking equipment offsite and that I must adhere to the requirements in this agreement.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to a Designated Safeguarding Lead or the IT Network Manager and report online material promoting radicalisation, terrorism or extremism.
- I understand I must report any breach of this policy or cyber-incident to the IT Network Manager or Headteacher or Senior Central Leader or the ICT Service Provider

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language, and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with this policy.
- I will ensure that my use of social media complies with provisions set out in this policy.
- When using a personal mobile or smart technology device to access social media I will ensure it is outside of school hours or on official breaks and always away from areas used by pupils.

- My digital interaction with pupils will be strictly limited to official applications.
- I will only communicate with parents/carers using official systems. Any such communication will be professional in tone and manner; I will remember that GDPR gives parents/carers the right to request access to any digital exchanges involving them or about them or their child.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- **I will not use the password(s) of another user to access school/CLP systems, and I will not share my own passwords(s) with other users**.

I understand that I am always subject to the Data Protection Act 2018, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988.

Staff / Volunteer Name:	
Signed:	**Date:**

Acceptable Use Agreement for Parents / Carers

Acceptable use of the ICT Network, school systems and internet:
Agreement for Parents / Carers
We ask that all parents are familiar with this Acceptable User Agreement and that they explain to their child(ren) why safe use of technology is important for everyone and so that pupils can learn in a positive and safe environment.

Coastal Learning Partnership's **IT and Communications Systems Policy** is available to read on the Coastal Learning Partnership website and can be found using the school website.

- I know that my child will be required to read and adhere to the Pupil Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that children will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet.
- I understand that my child's ICT activity will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.
- I will encourage my child to adopt safe use of the internet at home and will inform the school if I have concerns over my child's online safety or the online safety of any other child.
- I will encourage my child to undertake remote learning and will inform the school if I have any concerns over my child's use of online learning.
- I understand that, if my child brings personal mobile and smart technology devices into school (e.g., phones, cameras, smartwatches etc), the devices will be collected in, kept safe and returned at the end of the day; they should not be turned on until my child has left the school grounds.
- I understand pupils must not bring or wear AirTags, GPS trackers or other personal location-tracking devices during the school day or on educational visits unless expressly authorised by the Headteacher in exceptional circumstances.
- I have read and understood paragraph 24 of this policy and have explained to my child what this means for them.
- I understand that exceptions may be made for medical or learning reasons, and that if such exceptions are made by the Headteacher that my child must adhere to the conditions of use.
- Where a mobile / smart technology is used in school to monitor a medical condition or for learning, and is connected to the school internet because 4g/5g is not available, I understand that use of the device will be monitored by our filtering arrangements and that searches may trigger an investigation.
- I understand that my child's mobile or smart technology device may be confiscated by the school.
- I understand that my child is responsible for mobile or smart technology taken into school and that the school is not responsible for repair or replacement.
- I understand that the school can search for and delete images or files that are inappropriate from my child's personal IT device in line with *Searching, screening and confiscation* guidance.
- I understand that if I come to have digital images of children other than my own (for example, after taking pictures at a school event), I should not put them online without the explicit consent of the other children's parents/carers.
- I agree that any electronic communication, including email, from me to the school will be:
    - Related to non-urgent matters.
    - Directed to the right person (e.g., routine queries straight to the office, not a teacher).
    - Sent at appropriate times of the day / week (e.g., not to staff at evenings and weekends – emails can be sent at such times but preferably via the school's generic email address for the attention of the relevant teacher).
    - Reasonable in terms of the volume of emails sent.
    - Polite, courteous and respectful in tone.
    - Not demanding of a response in an unreasonable timeframe.
- I will ensure that any social media comments related to the school are polite and respectful and do not discuss members of staff or children in any negative way.

Appendix D: Pupil, Parent and Carer Code of Conduct for livestream learning

Pupil, Parent and Carer Code of Conduct for livestream learning:	
Name of pupil:	
Pupil: I understand that, if I am taking part in a livestream lesson, it is important for me to behave well: the usual classroom rules are the same online. **When I'm online, I understand that I am representing myself, my class and my school and I will ensure that everyone can be proud of me.** I will: • Be polite to staff and pupils. • Follow the rules that the adult in charge of the lesson sets. • Let the adult in charge of the lesson and an adult at home know if I see anything on the live stream that doesn't seem right. • Not take any photos or screenshots when I am using a live stream and I understand that sharing photos or screenshots is very serious. • Complete work and tasks to the deadline set by the adult in charge. • Seek help if I need it and let someone know if I'm not able to complete work. When at home I will: • Be in a space where an adult can easily check in on me. • Dress sensibly and wearing 'day time' clothes. • Be ready for lessons and log in at the right time. I understand that any live streamed remote learning sessions will be recorded to keep everyone safe **Parents and Carers** To enable my child to participate in and benefit from live lessons, I understand that my child's school has the following expectations of me and I will do my best to meet these expectations. I will: • Make sure that I have discussed all of the above points with my child and check that my child is adhering to them. • Make sure than an adult is nearby during live lessons and that this adult 'checks in' on my child from time to time. • Make the school aware if my child is sick or otherwise can't attend a lesson or complete work • Seek help from the school if my child or I need it. • Ensure my child is contactable during the school day and is ready to participate in live lessons • Be respectful when making any complaints or concerns known to staff. • Be mindful that other children might see or hear me and my child and anything in the background. • Make the school aware of any technical or hardware issues that might be a barrier to enabling my child to join live lessons.	
Signed (pupil name): **Signed (parent name):**	**Date:**

Appendix E: Video Conferencing - good practice

When hosting and taking part in video conferencing meetings, staff, Governors/Trustees, agency staff, volunteers and consultants working in schools should follow this guidance to ensure the meeting is both professional and effective and safeguards all participants and the Partnership.

MS Teams is the Partnership's video conference application of choice and meetings should be hosted using MS Teams by default. Our MS Teams is not enabled to conduct public meetings and cannot be searched for outside the ICT Network.

Good practice tips:

- Close email to prevent inadvertent sharing of emails;
- Have only documents intended for discussion or sharing open to prevent inadvertent sharing of documents;
- Ensure the recording facility is not enabled unless all attendees are made aware;
- Hosts should verify attendees before starting the meeting; they should admit only those who have been invited and reject those who have not;
- When at home, avoid attending the meeting in a bedroom or bathroom and use a neutral background or blurred background to provide privacy;
- Dress professionally;
- Use professional language;
- Don't sit in front of a window unless it has shutters or blinds to avoid appearing as a dark silhouette;
- If using personal devices such as a laptop then staff **must** first refer to Section 23;
- Consider background noise and conversations, and other people who might be in the room or vicinity;
- Do not make the meetings public. Invite participants directly using your contacts/address book or provide private links to the individual contacts.

When invited to meetings on other applications via Zoom, the same principles should be applied and staff should join the meeting via a browser.

In the event that an alternative platform is chosen to host a meeting, there should be a clear reason and further considerations detailed below should be followed:

- MS Teams is the Partnership's application of choice;
- Use a meeting code and password and only share these details with invited attendees and do so via email to ensure security;
- Do not make the meeting public. Invite participants directly or provide a private link;
- Connect directly to the people you want to call using your contacts/address book or provide private links to the individual contacts.
- Access should be via a browser, not app, unless using a partnership account.

Further guidance is available from the National Cyber Security Centre.

Appendix F: CLP ICT Network Key Contacts

Sue Grey	Head of Operations responsible for the CLP ICT network	01202 806155 / 07590 445115 sue.grey@coastalpartnership.co.uk
Sue Grey	CLP Data Protection Officer	01202 806155 / 07590 445115 DPO@coastalpartnership.co.uk
SchoolCare	ICT network professional services for all CLP schools including the O365 network.	Helpdesk: 0333 2402622 helpdesk@psdgroup.co.uk Managing Director and Account Manager: Steve Jones 01202 472997 / 07775 671759 E: steve@psdgroup.co.uk Senior Account Manager: Amber Hicks 01202 472991 / 07557 953313 E: amber@psdgroup.co.uk
Baden Powell & St Peter's CE Junior School	School Technician	Mark Branford Mark.Branford@BPSP.CoastalPartnership.co.uk 01202 743280 (school hours only)
Longfleet CE Primary School	School Technician	PJ Oulton PJ.Oulton@longfleet.coastalpartnership.co.uk 01202 673652/644441 (school hours only)

Appendix G: CLP Core Systems Matrix

At 27th February 2026

Communication & Engagement

Activity	Primary Choice(s)	Alternatives / Comments
Parent communications SMS, emails, in-app Newsletters	**MIS Arbor**	Dojo x 2 – under review Canva for newsletters? Juniper for newsletters?
Attendance letters	**MIS Arbor**	
Central SLT and Teams School SLTs and possibly other staff	**What's App – see Appendix I**	None
End of Year Pupil Reports	**MIS Arbor**	Likely to move to Insight
Parents' evening	**MIS Arbor**	
Payments (meals, trips, clubs)	**MIS Arbor**	
Staff engagement	**Intranet (SharePoint)**	
Website	**Juniper**	

Pupil management – teaching / learning / pastoral inc financial reporting where relevant

Activity	Primary Choice(s)	Alternatives / Comments
Admissions	**Applicaa** **Council system**	
Assessment/Reporting	**Insight**	
Attendance	**MIS Arbor**	
Behaviour	**MIS Arbor?**	Various platforms in use – under review due to inconsistent reporting and use of data
Behaviour rewards	**TrackIt** **Dojo**	Required to support behaviour policies
Classroom workflow / Assignments	**SharePoint** **Various edu apps**	
Pre-School	Tapestry, Famly, Blossom Early Years Transition Portal	Under review to achieve efficiency and consistency
Pupil reports and other reporting to parents	**Insight**	
Safeguarding	**MyConcern**	

SEND / Provision mapping	**Insight**	Provision MAP. All school moving towards Insight.
Trips	**EVOLVE**	None
Wrap around Care	**MIS Arbor**	

Corporate / Operational Functions

Activity	Primary Choice(s)	Alternatives / Comments
Asset & Estates / H&S Compliance / helpdesk	**Statlog**	
Catering orders	**Catering contractor**	
Data analytics	N/A at present, all in-platform	
Device Management (MDM)	**Intune for Education**	Jamf / Lightspeed – programme to migrate to InTune proposed
Finance	**The Access Group**	
Governance	**GovernorHub**	
HR/Payroll	**NEO**	
IT asset management	Hosted by IT professional services partner	
IT management software Inc Filtering & Monitoring, Backup	MS Entra InTune ESET Netsweeper Azure Backup Senso (from autumn 2026)	
IT Professional Services inc helpdesk	**SchoolCare**	
MIS (core)	**MIS Arbor**	
Occupational Health	**Everwell**	
Recruitment	**NEO**	
Risk & GDPR	(Not digital at present)	
Visitor Management	Various	

Appendix H: External disclaimer

Disclaimer: External individuals granted access to the CLP ICT network; namely agency supply teacher / SCITT teacher / appointed consultant.

Name:	**School or trust-wide based:**

I understand that I am to be given access to the CLP ICT network as though I were an employee to enable me to work effectively for Coastal Learning Partnership; this will involve the allocation of a profile allowing me to log on to ICT equipment and a @coastalpartnership email address.

I understand that being granted employee status on the ICT network will 1) enable me to access the school's network folders and software, 2) allow me to view and process personal data of pupils, parents and CLP employees, and 3) provide me with access to the CLP Intranet pages.

I understand therefore that I must I act in the best interests of the school I work in and Coastal Learning Partnership at all times.

I understand that I must keep all personal data secure and only use it for legitimate purposes and only share it for the purposes it is collected as set out in the policies named below and in our Privacy Notices.

I understand that I must be familiar with all CLP policies and in particular that I must understand the requirements for employees as set out in the:

- CLP Safeguarding and Child Protection Policy
- CLP IT and Communications Systems Policy
- CLP Data Protection Policy
- CLP Health and Safety Policy

I can confirm:

That I have signed the Acceptable User Agreement.

That if I am provided with IT equipment, I will sign a Loan of Equipment Agreement.

Signed:	**Date:**

Appendix I: Use of What's App for work purposes

WhatsApp may be used to support operational communication, routine coordination and urgent situations where timely communication is required. It is not an approved platform for formal decision-making or the exchange of confidential, sensitive, or personal information. All formal decisions, records, and business activities must be undertaken and recorded through Trust-approved systems and processes.

Use of WhatsApp for work purposes is voluntary unless specifically required as part of a defined operational role. Where WhatsApp is used for work-related communication, an alternative communication method will be made available where reasonably practicable to ensure that staff are not disadvantaged by choosing not to use the application on a personal device.

Staff using WhatsApp for work-related purposes must comply with the following requirements:

1. Purpose of Use
WhatsApp must only be used for operational communications, including brief updates, reminders, logistical arrangements, and urgent coordination of activities. It must not be used for conducting formal business processes or making decisions on behalf of the Trust.

2. Confidentiality and Data Protection
Staff must not share confidential, sensitive, or personal information via WhatsApp. This includes, but is not limited to:

- Pupil information;
- Safeguarding concerns or records;
- SEND information;
- Medical or health-related information;
- Human resources matters;
- Disciplinary or grievance matters; and
- Any other information subject to data protection or confidentiality requirements.

3. Record Keeping
Where a discussion on WhatsApp results in an action, instruction, decision, or matter requiring a formal record, the relevant information must be transferred promptly to an approved Trust system, such as email, Microsoft Teams, or another authorised platform.

4. Professional Conduct
All communications must be professional, respectful, and appropriate to a workplace environment. Staff should communicate in a manner that reflects the Trust's values and standards and should be aware that work-related messages may be disclosed as part of legal proceedings, audits, investigations, or information requests.

5. Security Requirements
Staff who access WhatsApp for work purposes must take reasonable steps to protect their device and account, including:

- Using a secure passcode, PIN, biometric authentication, or equivalent security measure;
- Keeping the application and device software updated; and
- Enabling two-factor authentication where available.

6. Work-Life Balance
Staff should avoid sending non-urgent messages outside normal working hours. The use of WhatsApp must not create an expectation that staff will read or respond to messages outside their contracted working hours, except where this forms part of an agreed role or emergency response arrangement.

7. Formal Decision-Making
WhatsApp must not be used to make, approve, or record strategic, financial, governance, staffing, risk-management, or other significant organisational decisions. Such matters must be considered and documented through the Trust's approved governance and decision-making processes.

8. Disclosure and Access Requests
Staff should be aware that work-related communications conducted through WhatsApp may be subject to disclosure in response to legal proceedings, audits, investigations, complaints, freedom of information requests (where applicable), subject access requests, or other lawful requirements.

9. Reporting Incidents
Any accidental disclosure of information, inappropriate use of WhatsApp, or suspected data breach must be reported immediately in accordance with the Trust's incident reporting and data breach procedures.

10. Group Management
WhatsApp groups established for work purposes must have a clear operational purpose. Group administrators are responsible for ensuring that membership remains appropriate and that individuals are removed promptly when access is no longer required.
This version is written in a policy style and should sit comfortably within an ICT Acceptable Use, Information Governance, or Staff Code of Conduct policy.