IT acceptable use policy

1. **Introduction**: This policy sets out the requirements with which you must comply when using the federation's IT and when otherwise using IT in connection with your job including:

   1.1 The federation's email and internet services.

   1.2 Telephones and faxes.

   1.3 The use of mobile technology on federation premises or otherwise in the course of your employment (including 3G/4G/5G, Bluetooth and other wireless technologies) whether using an academy, federation, or personal device.

   1.4 Any hardware (such as laptops, printers, or mobile phones) or software provided by, or made available by, the federation.

   1.5 This policy also applies to your use of IT outside federation premises if the use involves personal information of any member of the federation community or where the culture or reputation of the federation or any of its academies are put at risk.

   2. Failure to comply: Failure to comply will constitute a disciplinary offence and will be dealt with under the federation's disciplinary procedure.

2 **Property**: You should treat any property belonging to the federation with respect and reasonable care and report any faults or breakages immediately to the IT team. You should not use the federation's computers or other IT resources unless you are competent to do so and should ask for training if you need it.

3 **Viruses and other malicious code:** You should be aware of the potential damage that can be caused by computer viruses and other malicious code. You must not use, introduce, or operate any hardware, programmes, or data (including computer games) or open suspicious emails which have not first been checked by the federation for viruses.

4 **Passwords:** Passwords should be long; for example you could use a song lyric or a memorable phrase plus a number. Do not choose a password which is so complex that it's difficult to remember without writing it down. Your password should not be disclosed to anyone else. In addition:

   5.1 Your password should be difficult to guess. For example, you could base your password on something memorable that no one else would know. You should not use information which other people might know, or be able to find out, such as your address or your birthday.

   5.2 You must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any school account.

   5.3 Passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

   Please refer to the CLF Password and Encryption Policy located on CLiF for further details.

6. **Multi-Factor Authentication (MFA)**: You are requested to enrol a personal device to the multi-factor authentication system used by the federation, in order to ensure secure access to your personal information, such as staff payslips. If this poses a problem you should contact the IT helpdesk.

7. Leaving workstations: If you leave your workstation for any period of time you should take appropriate action and, in particular, you should log off and / or lock your computer by pressing the Windows key and "L."

7. **Concerns:** You have a duty to report any concerns about the use of IT in the federation to the principal, head of department or equivalent. For example, if you have a concern about IT security or pupils accessing inappropriate material.

8. **Other policies:** This policy should be read alongside the following:

- Code of Conduct
- Data protection policy for staff
- Information security for staff policy
- Password and Encryption policy
- Acceptable use policy for pupils
- Social Media Policy

Internet

9. **Downloading:** Downloading of any programme or file which is not specifically related to your job is strictly prohibited.

10. **Personal use:** The federation permits the incidental use of the internet so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the federation discovers that excessive periods of time have been spent on the internet provided by the federation, or it has been used for inappropriate purposes either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn without notice at the discretion of the principal or appropriate member of the Executive Team.

11. **Unsuitable material:** Unless deemed to be required for work purposes, and authorised accordingly, viewing, retrieving, or downloading of pornographic, terrorist or extremist material, or any other material which the federation believes is unsuitable, at any time, is strictly prohibited and constitutes gross misconduct. Internet access may be withdrawn without notice at the discretion of the Principal or appropriate member of the Executive Team whilst allegations of unsuitable use are investigated by the federation.

12. **Location services:** The use of location services represents a risk to the personal safety of those within the federation community, the federation's security, and its reputation. Staff are advised not make use of any website or application, whether on a federation or personal device, with the capability of publicly identifying the user's location while on federation premises.

13. **Contracts:** You are not permitted to enter into any contract or subscription on the internet (including through an App) on behalf of the federation or any of its Academies, without specific permission from the Principal or authorised line manager. This applies both to "free" and paid for contracts, subscriptions, and Apps. Where cost is incurred, authorisation must be gained from the relevant budget holder.

14. **Retention:** The Federation keeps a record of staff browsing histories in accordance with GDPR legislation.

Email

15. **Personal use:** The federation permits the incidental use of its email systems to send personal emails as long as such use is kept to a minimum and takes place substantially out of normal working hours. Personal emails should be labelled 'personal' in the subject header. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. The federation may monitor your use of the email system, please see paragraphs 24 to 28 below, and staff should advise those they communicate with that such emails may be monitored. If the federation discovers that you have breached these requirements, disciplinary action may be taken.

16. **Status:** Email should be treated in the same way as any other form of written communication. Anything that is written in an email is treated in the same way as any form of writing. You should not include anything in an email which is not appropriate to be published generally.

17. **Inappropriate use:** Any email message which is abusive, discriminatory on grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation, or religious belief (or otherwise contrary to our equal opportunities policy), or defamatory is not permitted. Use of the email system in this way constitutes gross misconduct. The federation will take no responsibility for any offence caused by you as a result of downloading, viewing, or forwarding inappropriate emails.

18. **Legal proceedings:** You should be aware that emails are disclosable as evidence in court proceedings and even if they are deleted, a copy may exist on a back-up system or other storage area.

19. **Jokes:** Trivial messages and jokes should not be sent or forwarded to the email system.

20. **Contracts:** Contractual commitments via email correspondence are not allowed without prior authorisation of the principal or appropriate senior manager.

21. **Disclaimer:** All outbound correspondence by email contains the federation's disclaimer.

22. **Data protection disclosures:** Subject to a number of limited exceptions, potentially all information about an individual may be disclosed should that individual make a subject access request under GDPR legislation. There is no exemption for embarrassing information (for example, an exchange of emails containing gossip about the individual will usually be disclosable). Staff must be aware that anything they put in an email is potentially disclosable.

Monitoring

23. The federation regularly monitors and accesses its IT system for purposes connected with its operation. The federation IT system includes any hardware, software, email account, computer, device, or telephone provided by the federation or used for federation business. The federation may also monitor staff use of the federation telephone system and voicemail messages. Staff should be aware that the federation may monitor the contents of a communication (such as the contents of an email).

24. The purposes of such monitoring and accessing include:

25. To help the federation with its day to day operations. For example, if a member of staff is on holiday or is off sick, their email account may be monitored in case any urgent emails are received.

26. To check staff compliance with the federation's policies and procedures and to help the federation fulfil its legal obligations. For example, to investigate allegations that a member of staff has been using their email account to send abusive or inappropriate messages.

27. Monitoring may be carried out on a random basis, and it may be carried out in response to a specific incident or concern.

28. The federation also uses software which automatically monitors the federation IT system (for example, it would raise an alert if a member of staff visited a blocked website or sent an email containing an inappropriate word or phrase).

29. The monitoring is carried out by a number of systems. If anything of concern is revealed as a result of such monitoring, then this information may be shared with those investigating the concern and any relevant senior management. This may result in disciplinary action. In exceptional circumstances concerns will need to be referred to external agencies such as the police.