Spring Trust

No Barriers to Excellence

Ambition Collaboration Equity

# E-Safety and Acceptable Use Policy

| Version | Name | Date |
|---|---|---|
| V1.6 | Rob Taylor, Chair of FARCO | June 2020 |
| V1.7 | Rob Taylor, Chair of FARCO | November 2021 |
| V1.8 | Rob Taylor, Chair of FARCO | November 2022 |
| V1.9 | John Cliff, Chair of FARCO | October 2023 |
| V1.10 | Michael Ellis, Chair of FARCO | October 2024 |
| V2 | Michael Ellis, Chair of FARCO | September 2025 |
| | | |

# E-Safety and Acceptable Use Policy

## The aims of this policy are to:

- Ensure that pupils benefit from all digital opportunities provided by the schools in a safe and controlled manner, in accordance with the Trusts External Communications Policy.
- Ensure that all staff benefit from internet access, with clear guidance on safe and acceptable use.
- Make staff and pupils aware that internet use in schools is a resource and a privilege. If the terms are not met, then that privilege will be taken away.
- Provide guidance to staff and pupils about the acceptable use of mobile technologies, both the school's and personal items that are brought into school.
- To set out the Trust expectations of the use of technology in order to comply with the General Data Protection Regulations (GDPR).

## Acceptable Use Statement

The computer system is owned by the Trust. "The computer system" means all computers and laptops and associated equipment belonging to any school, whether part of the Trust's integrated network or stand-alone, or taken offsite.

Professional use of the computer system is characterised by activities that provide children with appropriate learning experiences or allow adults to enhance their own professional development. The Trust recognises that technologies such as the internet and e-mail will have a profound effect on children's education and staff professional development and this Acceptable Use Policy has been drawn up accordingly. This policy has been drawn up with reference to:
The Data Protection Act (2018); the GDPR (2018); the Computer Misuse Act (1990); the Regulations of Investigatory Powers Act (2000); the Lawful Business Practice Regulations (2000) and relevant DfE guidance (including the latest Keeping Children Safe in Education document) and should be read in conjunction with the Trust Child Protection and Safeguarding policy.

The Trust reserves the right to examine or delete any files including personal files and emails that may be held on its computer systems or to monitor any internet sites visited.

All 'users' (defined as members of staff, students on placement, regular supply teachers and Trustees) must be aware of and sign a copy of the 'Acceptable Use Agreement' which will be kept on file. This applies to all of the above groups who are accessing the computer network, not just those issued with Trust IT equipment.

All users should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programmes. Reference should also be made to the Trust External Communications Policy.

All children must be made aware through class discussion and assemblies of all the important issues relating to acceptable use, especially the monitoring of internet use. Safe use will be covered within the computing curriculum, to allow children to feel safe when online both in school and at home.

Parents will provide consent for pupils to use the internet, as well as other ICT technologies, as part of the e-safety Acceptable Use Agreement form at the time of their child's entry to school. Children will also sign the same agreement at this time regarding 'rules of appropriate use'. They will sign a second, more detailed 'rules of appropriate use' form on progression from KS1 to KS2. These agreements can be found at the end of this document.

Parents/carers are required to sign relevant documentation agreeing to the Trust controls regarding the safeguarding of pupils and the appropriate use of any digital equipment before it is taken off-site.

# Internet Access Policy Statement

All internet activity should be appropriate to staff professional activities or the children's education:

- Access is limited to the use of authorised accounts and passwords, which should not be made available to any other person;
- The internet may be accessed by staff and children (when supervised by an adult) throughout their hours in school;
- Activity that threatens the integrity of the Trust's computer systems, or that attacks or corrupts other systems, is prohibited;
- Users are responsible for all e-mails sent and for contacts made that may result in e-mail being received. Due regard should be paid to the content. The same professional levels of language should be applied as for letters and other media;
- Use of the Trust's IT facilities for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is prohibited;
- Use of the Trust's IT facilities for any kind of social networking is prohibited, excepting official school business;
- Copyright of materials must be respected. When using downloaded materials, including free materials, the Intellectual Property rights of the originator must be respected and credited. All material saved on the Trust's IT network is the property of the Trust and making unauthorised copies of materials contained thereon maybe in breach of the Data Protection Act, General Data Protection Regulations, Individual Copyright or Intellectual Property Rights;
- Posting anonymous messages and forwarding chain letters is prohibited;
- Sending or posting any material with malicious content will be taken very seriously and sanctions will be applied as appropriate.
- The use of the internet, e-mail, or any other media to access or send inappropriate materials such as pornography, racist or any other offensive material is forbidden and appropriate sanctions will be applied;
- All web activity will be monitored as necessary to ensure no inappropriate content is being accessed.
- Children will be given guidance as to the appropriate use of the internet.
- The teaching of Internet safety is included in the Trust's Computing Scheme of Work and/or is covered in PSHE lessons, but all teachers within all year groups should be including Internet safety issues as part of their discussions on the responsible use of the Trust's computer systems;

- All children must understand that if they see an unacceptable image on a computer screen, they must turn the screen off and report immediately to a member of staff.
- Staff must report any unacceptable images to the Headteacher. The screen must be turned off immediately and children involved must be given a reminder on procedures for reporting inappropriate images.
- Staff should not engage in any social networking (eg: Facebook) with current or former pupils.
- When setting work for pupils to complete remotely all staff will ensure that the content of any links or websites suggested for pupils to access is age appropriate.

# Internet Access and System Monitoring

Keeping Children Safe in Education obliges academies to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

Across the Trust, the internet connection is provided by LGfL. This means we have a dedicated and secure, safe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in academies. Unfortunately, inappropriate materials will inevitably get through any filtering system, and any inappropriate material must be reported to the Headteacher. While the Trust complies with all Filtering and Monitoring requirements as set out in KCSIE, Spring Trust cannot accept liability for material accessed, or any consequences of internet access. Conversely, sometimes appropriate websites need to be unblocked if deemed useful for children's learning. Any requests shall be passed directly to the IT Support company to unblock the requested site. High level monitoring of website access is also undertaken by LGfL and logs can be obtained if necessary.

Both staff and pupils should be aware that the Trust may exercise its right by electronic means to monitor the use of the Trust's computer systems. This includes the monitoring of websites and the interception of e-mails in circumstances where it suspects that unauthorised use of the Trust's computer system is or may be taking place. No separate record of personal data following such monitoring will be retained unless there are any potential disciplinary/illegality issues.

# Photographs and Video

Children's photographs/videos may be used on the schools' websites. Please refer to the Trust Data Protection Policy and the Trust Photographs and Video Policy for further information on this area. Adults must only use equipment provided or authorised by the Trust to make/take images and must not use personal equipment, mobile telephones or any other similar devices to make/take images. A minimal number of SLT staff (with prior authorisation/risk assessment) may use their personal mobile phones solely to allow uploading of information to promote the school's social media accounts.

# Prevent Duty

Safeguarding Children and Young People Vulnerable to Violent Extremism.

Protecting children from the risk of radicalisation is part of the Trust's wider safeguarding duties and is similar in nature to protecting children from other forms of harm and abuse. There is a statutory duty to have due regard to prevent children from being drawn into terrorism and the advice in Prevent Duty Guidance for England and Wales 2015 should be followed. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism. There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. As with managing other safeguarding risks, schools should be alert to changes in children's behaviour, including online behaviour that could indicate that they are in need of protection.

School staff should use their professional judgement in identifying children who might be at risk of radicalisation and act proportionately. This may include making a referral to the Channel programme (Keeping Children Safe in Education, Department for Education). Please refer to the Child Protection and Safeguarding Policy for more information.

# Sanctions

Transgressions of this Policy by pupils will be dealt with in a range of ways, including removal of internet access rights; computer system access rights; meetings with parents or even exclusion; in accordance with the severity of the offence and the Trusts Behaviour Policy.

Breaches of this Policy by staff will be reported to the relevant Headteacher and will be dealt with according to the Trust's disciplinary policy, or through prosecution by law.

A log of any misuse or abuse of computer systems will be kept on the relevant personnel file.

# System Security

The following measures are in place for all users in order to protect the Trust network and systems and to mitigate risk:-

- Google multi factor authentication (MFA), also known as 2FA, must be enabled.
- Password resets must be validated either by phone call or line manager approval before they are actioned.
- Documents should be stored on a relevant shared drive
- User accounts will be removed from the system when an employee leaves.
- Personal devices should not be used for work purposes.
- Personal email and personal Google accounts should not be accessed on work devices.

# APPENDICES

## Appendix 1 - Acceptable Use Agreement – EYFS/KS1

| Think before you click! | |
|---|---|
| S | I will only use the internet and email with an adult. |
| A | I will only click on icons and links when I know they are safe & I have been told to. |
| F | I will only send friendly and polite messages to people I know. |
| E | If I see something I don't like on a screen, I will always tell an adult immediately. |

My name:
My signature:
My parent's/carers name:
My parent's/carers signature:

# Appendix 2 - Acceptable Use Agreement – Pupils KS2

We use the school computers and internet connection for learning. These rules will help us to be responsible users who will endeavour to keep ourselves and everyone else safe.

Using the Computers

- I will only use my class login, unless my teacher has asked me to use a different one.
- I will not look at or delete other people's files.
- I will not bring in or use data storage devices from home.

Internet

- I will ask permission from my teacher before using the internet.
- I will report any unpleasant material to my teacher immediately because this will help protect myself and other pupils.
- I understand that the school may check my computer files and monitor the internet sites I visit.
- I will make sure I use the right kind of websites when searching for information to complete school work at home.

Digital Communication

- I will ask permission from my teacher before using our approved email system.
- I will not give my personal information to anyone over the internet (at home or at school).
- If I see anything I am unhappy with, or I receive messages I do not like, I will tell a teacher immediately.
- I understand that any messages I receive or send leave a digital footprint, reflect on myself and my school and may be read by others.
- The messages I send will be light, bright and polite.
- I will follow any rules put in place about video meetings with my teachers when I am doing school work at home.

Digital Technology

- If I use any digital equipment belonging to the school (such as chromebooks/digital cameras), I will always treat it with care and respect, and report any breakages or accidents immediately to the nearest adult.

**I understand that if I deliberately break any of these rules then I could be stopped from using the internet or computers.**
**My parent/s has also read and agreed to help me follow these rules.**

My Name: Parent's/Carers Name:

My Signature: Parent's/Carers signature:

# Appendix 3 - Acceptable Use Agreement – staff and other users

The computer system network, laptops and other devices are owned by the Trust and may be used by children to further their education and by staff to enhance their professional activities including teaching, research, administration and management. The Trust's Acceptable Use Policy has been drawn up to protect all parties – the pupils, the staff and the schools/Trust.

The Trust reserves the right to examine or delete any files including personal files and emails that may be held on its computer system or to monitor any Internet sites visited.

All users who access the internet or use Trust devices should sign a copy of this Acceptable Use Agreement and return it to the Trust's HR department to keep on file.

- All internet activity should be appropriate to staff professional activity or the children's education;
- Access should only be made via the authorised user account;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;
- Internet use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Copyright of materials must be respected;
- Posting anonymous messages and forwarding chain letter emails is forbidden;
- As e-mail can be mistakenly forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
- Use of the network to access or send inappropriate materials such as pornographic, racist or offensive material is forbidden and sanctions (such as police involvement) will apply;
- Staff should only use school digital media to photograph or record images of children for school use only.
- Staff should not create or keep any personal files on Trust systems or computers as these are for Trust/school business use only.
- The Trust Data Protection Policy, Data Protection Act 2018 and the General Data Protection Regulations must be followed in accordance with the Trust Privacy Notices.
- Family members or other 'non-Trust' users must not be allowed to access Trust computer systems or use Trust IT facilities without the agreement of the relevant Headteacher.
- Staff must ensure they comply with the Trust expectations in relation to video conferencing meetings (as detailed in the Trust External Communications Policy) with other staff members, parents/carers, pupils or any external parties.

**IT Security**

- No Trust/school files should be stored on personal devices and personal devices should not be used for work purposes.
- The transferring of files onto the Trust's network must be carried out using Google Drive or an encrypted memory stick.
- We have approved educational web filtering across our wired and wireless networks.

- We follow approved methods (such as LGfL USO-FX, or Egress) for the internal and external transfer of any special category data.
- We expect all users to undertake house-keeping checks annually to review, remove and destroy any files and documents that no longer need to be stored.
- We require staff to lock their screens when leaving their computer, but also enforce lock-out after 10 minutes of idle time.
- For Trust devices used off-site we use Google Workspace with its 2-factor authentication for remote access into our systems.
- All staff are required to enable Google multi-factor authentication.
- We use LGfL AutoUpdate for creation of online user accounts for access to broadband services.
- All servers are in lockable server room locations (with the exception of one site which is logistically unable to offer this) and managed by DBS-checked staff.
- All data is backed up remotely using a reputable off-site company.
- Any cloud hosted data is held with third parties that comply with the Trust cloud service provider expectations.
- We comply with the WEEE directive on IT equipment disposal, by using an approved disposal company. For systems where data has been held (such as servers or photocopiers), we get a certificate of secure deletion.

**Password Expectations**

Passwords shall:

- consist of a minimum of 8 and a maximum of 16 characters and contain characters from the following 3 categories:
  Uppercase characters (A - Z)
  Lowercase characters (a – z)
  Numbers (0 – 9)
- Expire after 90 days (Windows will notify users 14 days prior to the password expiring);
- Not be re-used (15 previous passwords will be remembered).

**User accounts will:**

- be locked out after 5 invalid logon attempts
- remain locked for 30 minutes or until a member of IT unlocks the account.

**Emails**

- No non-Trust email accounts should be used by users for the sending and receiving of emails relating to Trust business.
- Never open email attachments from a sender you don't recognise. Just delete the email.
- Don't open attachments from a sender you know if it seems unusual - this is often the way viruses spread.
- Check the senders name carefully: the practice of providing false information in message headers is a growing problem. This is also known as spoofing. For example, a message might indicate that it is from Eric Lang at Alpine Ski House (eric@alpineskihouse.com) when it is actually from a bulk email service that promotes schemes to get rich quickly. Therefore, don't just rely on the display name but look at the email header address.
- Check for obvious spelling mistakes – often a sign of malpractice

- Don't click on links within emails unless you're sure they are OK.
- Be very cautious of any email which says it is urgent or is in some way alarming.

**Other**

- Non-Trust devices must connect to the Trust's network via the secure Guest wifi network, and not the main Trust network.
- Any non-Trust device which might be used for Trust purposes, for example by Trustees, must:-
  1. have anti-virus software installed by the owner;
  2. be password protected with a strong and regularly changed password (see Password Expectations above);
  3. not have any Trust data saved onto it which is considered 'personal' or 'special category' as defined by the GDPR.
  4. If point 3 is unavoidable in exceptional circumstances the data must be password protected and stored securely. The 'personal' or 'special category' data must be deleted from the device at the earliest possible opportunity.

The Trust may exercise its right by electronic means to monitor the use of the Trust's computer systems, including the monitoring of websites, the interception of e-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the Trust's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

I agree to follow the guidelines for computer and Internet use as outlined above:

Name: Signed: Date:

# Appendix 4 - Staff Equipment Contract

Name: Job Title:

I confirm that I have been issued with the following Trust equipment – please tick as appropriate:

| **Equipment being issued** | **Tick** | **Returned at end of employment (Please tick and date)** |
|---|---|---|
| Laptop / Chromebook / Tablet / Ipad – delete as appropriate<br><br>**Asset number:**_____ | | |
| Power Supply | | |
| Encryption Key | | |
| Carry case/protective case | | |
| Mobile phone (model_____)<br>Telephone number: | | |
| Keys - detail which school and what keys are for: | | |

With respect to the equipment I have been issued:

- I understand that the equipment is the property of Spring Trust and will be recalled whenever the Trust deems necessary, and will be returned if I am no longer employed by the Trust. I understand that I must comply immediately if such a request is made.
- I understand that the security of ICT equipment is my responsibility and I could be liable for the cost of replacement should they be stolen from any location where I have not ensured appropriate security.
- I understand that any data breaches involving Trust equipment must be reported as a matter of urgency.
- I understand that damage incurred to the laptop or power supply is covered by insurance and I would not be liable for the cost of replacement or repair. This includes damage incurred at school or home.
- I understand that the expected 'working life' of the device (if cared for properly) is in excess of four years and I will take all due care of any equipment provided to me.

With respect to all other ICT equipment:

- I understand it is my responsibility to maintain the integrity of my network password.
- I fully understand that the installation of software or hardware unauthorised by the Trust, whether legitimately licensed or not, is expressly forbidden.
- Encrypted USB memory sticks (provided by the Trust) will only be used if no other option is available for the transfer of files. The use of unencrypted memory sticks is not acceptable in any scenario, and their use may result in disciplinary action.
- If I need to contact the IT support department to report a problem with any school-based ICT equipment, I understand I can e-mail servicedesk@platform365.co.uk

Please send completed document to hr@springpartnership.co.uk who will upload a copy onto your Edupay file.

I agree to abide by this staff ICT equipment contract.

Signed: Date:

Spring Trust

Registered Office: Elmstead Wood Primary School,
Castlecombe Road, Mottingham, London SE9 4AT

**T:** 0203 837 8637
**E:** contact@springpartnership.co.uk

Spring Trust