Leading Learning Trust – Online Safety Policy

This policy is applicable to both Selwyn Primary School and Portway Primary School.

Reviewed to ensure UK GDPR compliance, and again in light of 1:1 device provision

Date reviewed:	November 2021
Reviewed by:	Leadership team
Next review planned for:	October 2024
Policy ratified by CEO (as per Scheme of Delegation):	December 2021

Leading Learning Trust

Selwyn Primary School and Portway Primary School are part of the Leading Learning Trust.

Contents

1. - OVERVIEW OF THE POLICY MANAGEMENT PROCESS

1.1. Document history

Date	Document title	Version
31/10/16	Initial draft of the policy released and approved by the EHT - released as a Portway/Selwyn applicable policy.	1.0
Nov 2017	Policy updated from Selwyn/Portway applicable to a Leading Learning Trust document. All the relevant changes have been made in the text to reflect this. Review of the policy in line with GDPR/Data Protection Act 2018 compliance. **1.2.** Review also requires the input of the DPO (Data Protection Officer) as the policy contains personal data. **Introduction** - rewritten entirely - links to the ICT Acceptable Use Policy and Agreement and to the GDPR. **Website content** - new Photography Policy referenced; confirmation of strict password protected access to the school websites. Note that reference to supply of this form at admissions has been removed (we are reviewing how we ensure sign-up to these arrangements). **Safety of Internet access** - reported to the Trust ICT Network Manager; information re social networking sites. **Security of the system** - added in use of Google Drive and impact of this change **How are staff and children consulted** - reference to the ICT Acceptable Use Policy and Procedure at admissions has been removed (we are reviewing how we ensure sign-up to these arrangements). **How is personal data protected** - updated to reflect the use of G Suite for Education and all documentation stored on Google	2.0

	Drive. Also the fact that the data centres used by Google in their G Suite for Education product are within the EU. Note that further information re all collection and processing activities is available at the registered office of the trust, at Selwyn.	
Sept 2020	**2.11.** - Changed "If staff or pupils encounter unsuitable content or sites then these sites will be reported to the Trust ICT Network Manager or his apprentice" to "If staff or pupils encounter unsuitable content or sites then these sites will be reported to the Trust IT Team"	2.1
Dec 2021	**Review in light of 1:1 device provision** - Data protection team updates provided as comments - for IT Director and CEO review - 1:1 provision specific section added - section 2.19 in this version - Removed references to BECTA and NCH New section reviewed by IT Director and Trust Safeguarding Lead	3.0

1.2. Review and approval

The Leading Learning Trust trustees have overall responsibility for the policy.

The CEO is responsible for the operation of the policy within the schools, as well as for the maintenance of a record of concerns raised in accordance with this policy and the outcomes.

This policy is reviewed every 3 years by the School Leadership Team, and is then ratified by the CEO. As this policy references personal data, it has been reviewed as part of our GDPR (General Data Protection Regulations) project. In addition, our Data Protection Officer is part of every review of this policy.

2. - THE POLICY

2.1. Introduction

At the Leading Learning Trust, we believe that the ability of our children to access and to use new and evolving technologies is a crucial part of their education. However, as is the case with all technologies, we are aware of the potential that exists to abuse these technologies.

To ensure that children are able to benefit from the latest technology, and know how to keep themselves safe online, the use of IT systems is integrated across all our teaching and learning at our schools.

Both children at Selwyn and Portway Primary School, as well as all adults working at the Leading Learning Trust read and agree to our *ICT Acceptable Use Policy and Agreement*, both of which are available on the Selwyn and Portway websites. Appropriate training is provided, and leadership structures ensure that our systems are safe, and always fit for purpose. The roles and responsibilities of all staff and school leaders are clearly detailed in the Acceptable Use Policy and Agreement.

Children and staff are also made aware of this *Online Safety Policy*, which is available on both the Selwyn and the Portway websites on the Behaviour pages; useful external online safety links are provided in the same place. Online safety is also referenced in our *Behaviour Policies*, as well as in our *Early Help, Safeguarding and Child Protection Policies*, all of which are available on the Selwyn and the Portway websites.

Online safety includes both access to the internet and electronic communications such as mobile phones. It highlights the need to educate pupils and staff about the benefits and risks of using technology, and provides safeguards and awareness for users to help them to control their online experience.

2.2. Aim

This policy aims to ensure that all children are aware of how to use the Internet and other electronic communications devices safely.

It should be read in conjunction with the ICT Acceptable Use Policy and Agreement, in which all key roles and responsibilities are outlined. The Trust has in place Acceptable Use Agreements for KS1 and KS2 children, which have been developed to ensure they are accessible to the relevant groups. The Trust also has an Acceptable Use Agreement and associated policy in place, which all trustees, governors, staff and volunteers (ie. all adults

using the Trust's systems) complete as part of their onboarding with the Trust. This Agreement and the policy are kept under close review by the IT Director, given the rapidly changing IT landscape.

The Trust has a separate Cyber Security Policy in place, approved by the Trust Board.

2.3. Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the efficacy of the trust's management processes.
- Internet use is a necessary tool for learning for pupils and staff. It is an entitlement for children who use it responsibly.
- It is a requirement of the National Curriculum orders for ICT, and is indicated as a Key Skill in other subject orders.
- The internet is an essential element in 21st century life for education, business and social interaction; it is thus essential that pupils are introduced to it, under supervision, at school.

2.4. How does Internet use benefit education?

- Access to world-wide educational resources including museums and galleries.
- Inclusion in the wider network of schools across the UK.
- Educational and cultural exchanges between pupils worldwide.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to educational materials and effective curriculum practice.
- Communication with the LA advisory and support services, professional associations and colleagues.
- Access to key educational and monitoring resources.
- Home-school links communication is improved by direct emails and website Information.
- The current Covid-19 pandemic has demonstrated the crucial role that the Trust's integrated IT Strategy has played in ensuring that children are able to continue their education throughout the series of lockdowns.

2.5. How can Internet use enhance learning?

- Internet access is filtered appropriate to the age of pupils.
- Pupils will be given clear objectives for Internet use, to support the work that they are doing across the curriculum.

- Internet use is planned to enrich and extend learning activities. Access levels are reviewed to reflect the curriculum requirements and age of pupils.
- Staff will select sites that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in taking responsibility for their own Internet access.
- As noted above, the Covid-19 pandemic has thrown the crucial role of IT in learning into sharp relief. The Trust has continued to use a number of strategies developed during the pandemic to enhance provision in a number of areas (eg. recordings of the work of SEND children to share with parents and carers).

2.6. How can pupils learn to evaluate Internet content?

- The evaluation of online content is a part of every subject.
- Pupils will be taught ways to validate information by cross-checking before accepting its accuracy.
- Pupils will be made aware that the author of a web page or an e-mail might not be the person claimed.
- Pupils will be encouraged to inform a member of staff immediately if they witness any content that makes them feel uncomfortable.

2.7. How is email managed?

- E-mail will only be used by pupils for educational purposes.
- Pupils will learn to email using the class email provided by LGfL (London Grid for Learning). Nominated contacts are able to access these accounts and monitor activity within a school context and also remotely.
- Staff should use the official school email provided by LffL for all school contacts.
- All messages should be polite and responsible.
- Pupils must immediately inform a member of staff if they view an offensive or unpleasant e-mail or other online or digital communication or content.
- Pupils must not reveal any personal details of themselves or others in emails, or arrange to meet anyone without specific permission. Staff also have access to email, although they are discouraged in using personalised email accounts in school. For further information relating to staff email accounts, reference can be made to the school *ICT Acceptable Use Policy and Agreement*.

2.8. How is content on our school website managed?

- The CEO/Head teacher has overall editorial responsibility and ensures that content is accurate and appropriate.
- Access to editing the school websites is strictly controlled and is only possible by authorised users.

- The website is audited annually, and the results reported to the Trust Board, to ensure that information remains current and that all compliance requirements are met.
- Along with ensuring that compliance requirements are satisfied, Head teachers review the website on an ongoing basis to ensure that content is both useful and accessible to parents.
- The contact details on the website are the school address, e-mail and telephone number. No details of pupils' personal details are published.
- In all instances, photographs used on the websites will be unnamed. Group shots will be used in preference to images of individual children.
- We have a Leading Learning Trust *Photography Policy*, which has been put in place as part of our compliance with the GDPR (General Data Protection Regulations). This is available on the Selwyn and Portway school websites.
- The *Photography Policy* allows parents to specify their preferences around the taking and display of photographs of their children.

2.9. How is Internet access authorised?

- Internet access is a necessary part of the National Curriculum. It is an entitlement for pupils based on responsible use.
- Internet access will be granted to classes, groups and individuals as part of the curriculum schemes of work. Pupils will have been informed of responsible internet use. All internet use is strictly under adult supervision and as a result of specific, approved on-line materials.
- As noted in Section 2.2, the Trust has age-appropriate Acceptable Use Agreements in place - ie. as soon as children are introduced to the internet, they are made aware of acceptable behaviours.

2.10. How are risks assessed?

- Across the Leading Learning Trust, we ensure that we take all reasonable precautions to ensure that users can only access appropriate content. However, due to the global and connected nature of Internet content, it is not possible to guarantee that unsuitable material will never occur via a school computer. Selwyn and Portway Primary School cannot accept liability for the material accessed, or any consequences resulting from Internet use. Staff and children are made aware of how to report unsuitable materials or on-line incidents.
- Methods to identify, access and minimise risks will be revised regularly. The Leading Learning Trust has an integrated Health and Safety Management System in operation across the trust - and risk assessment methodologies are in place.
- Staff, parents, governors and members of the trustee board will work together to ensure that every reasonable measure is being taken.

- As at October 2021, the Trust has in place a Cyber Security: policy, certification, risk mitigation and incident management plan in place.
- As part of the risk mitigation strategy, the Trust has earmarked funds to purchase devices to allow the safe and appropriate use of 2 factor authentication for all Trust accounts.

2.11. How will the school ensure that Internet access is safe?

- Pupils will be informed that Internet use will be supervised and monitored.
- All Internet access is filtered by systems put in place by LGfL (see above).
- If staff or pupils encounter unsuitable content or sites then these sites will be reported to the Trust IT Team.
- Staff should be aware that bullying can take place through social networking out of school and the problems associated with this can come into school.
- All staff are aware that access to social networking sites (e.g. Facebook, Twitter, Instagram) have a minimum age of 13 years, although we keep this age specification under review as it may vary in future by social network. Guidance is regularly provided to parents on this issue, and is widely available on both school websites and online.

2.12. How will the security of the school ICT systems and the data held on them be maintained?

- The security of the school information systems is monitored constantly and will be reviewed regularly. Details of these arrangements are available in the Trust's Data Security Policy.
- Virus protection is supplied by LGfL and certain websites which are naturally blocked due to sensitive content or keywords. Teachers have some access to sites such as these through a USO override log in. However, this infrequent activity is logged through LGfL, and is not available to children.
- Portable media (hard drives, USB drives and so on) *may not* be used by pupils without specific permission. This includes the use of mobile phones. Children are discouraged from bringing mobile phones to school. However, those with a specific need for a mobile phone agree to clear criteria set out for use of the device (for instance, the use of phones is not permitted during school hours). Teachers do not use mobile phones for the taking of pictures of children at school, or for storage of school data.
- Portable media used by staff needs to be checked for viruses. Staff should not be permanently storing any sensitive data outside the school environment. Relevant files need to be deleted after use.
- Technical advice is to be sought before any downloads of programs/macros unless they come from specific known and named sources.

- The Trust uses Google Workspace which ensures that all school data is encrypted.
- The Trust's Records Retention Policy (and associated 'managed housekeeping' of all electronic files) ensures that the UK GDPR (UK General Data Protection Regulation) 'minimisation by design' principle is adhered to. Whilst the Regulation refers to personal data, best practices developed by the Trust to safeguard personal data are used to manage all electronic data held on Trust systems.

2.13. How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be dealt with by the CEO/Head teacher or the School Leadership Team.
- The Leading Learning Trust Complaints Policy is available on our school websites, and details how parents should seek to resolve any concerns or complaints. A copy is also always available from the school office.
- At Selwyn and at Portway, we work closely with parents and with children to ensure that any concerns are addressed.
- Actions within school may include one or more of the following:
    - discussion with teacher or the CEO/ Head teacher
    - parents informed
    - removal of Internet or computer access for a period of time.

2.14. How are children taught about online safety?

- Children are consulted about technology usage through annual surveys.
- Units of work consolidate the school's online safety message, and the ethos and rules for Internet use have had extensive input from the children.
- Displays around the school and specifically in the ICT suite consolidate the whole school message around online safety.

2.15. How are staff and pupils consulted?

- Online safety rules are explained and discussed with classes by teachers at a level appropriate to the age of the pupils.
- Online safety training will be developed, possibly based on CEOP (Child Exploitation and Online Protection Centre) materials and these will be embedded within ICT Schemes of Work and / or RSHE and wellbeing curriculum through the creative curriculum (online safety day is held as an annual event to convey the message of online safety).
- Pupils in KS1 and KS2 complete the *ICT Acceptable Use Policy and Procedure*. Rules for Internet use are posted near computers with Internet access.
- All staff have access to this policy, and are aware of its contents.

2.16. How is parents' support enlisted?

- A partnership approach with parents is part of the ethos at Selwyn and at Portway Primary School.
- Parents' attention will be drawn to the Online Safety Policy when the child starts school, and they will be notified that it is available on the school websites.
- Advice for parents will be available on the school website from agencies such as, Action for Children, BBC and CEOPS (Child Exploitation and Online Protection Centre); this advice is kept under review and is subject to regular updates.
- At Selwyn Primary School, all parents will be asked to sign the parent/pupil agreement when they register their child with the school.

2.17. How are emerging technologies managed?

- These will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Any resource preparation, completed by staff at home, which involves the use of pupil images, must be prepared and stored on Google Drive.
- Digital imaging systems e.g. video-conferencing and web cam, will be appropriately supervised according to the pupils' age.
- The Trust's compliance with UK GDPR (referenced earlier) ensures that a Data Impact Assessment is carried out as part of standard practices when reviewing the introduction of any new policy or process that entails new technologies. Although these assessments are specifically in place to safeguard personal data, they are used whenever new technologies are considered for implementation.

2.18. How is personal data protected?

- Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998, the UK GDPR (General Data Protection Regulation) and the Data Protection Act 2018. This data is stored on Google Workspace, and is encrypted. As a data processor, Google's policies and processes are GDPR compliant. Further detail regarding this compliance is available from Google.
- Google Drive is configured to ensure Shared Drives and permissions are appropriately configured, and kept under constant review.
- Personal data is only kept for the time needed and then it will be disposed of in accordance with our Records Retention Policy.
- The Trust has a Privacy Notice in place for children, parents, staff, governors and trustees. These are provided at the point that data is collected, and explain the purposes for which it is used, and how it will be processed, shared and retained. Consent for any additional processing activities is separately sought and appropriately documented.

- Further information regarding the Leading Learning Trust's collection, processing and disposal of personal data is available via the registered office of the trust, at Selwyn Primary School, as part of the trust's Records Retention Policy.

2.19. One to one device provision at the Leading Learning Trust

The Trust has a comprehensive IT Strategy in place, and ambitious plans to ensure that our children have the best possible access to digital technologies to enhance their learning and prepare them for a digital world.

As part of this strategy, and supported by the processes outlined in this policy and in place across the Trust, the provision of devices for children in years 5 and 6 at Portway and years 3 and 6 at Selwyn, will be implemented in early 2022.

The issue of these devices has been made possible as part of the IT Strategy, and by the funding approved by the Trust Board. Existing policies, systems and processes, supported by the IT Director and his team, make this provision possible in a safely managed way.

The Trust has developed an appropriate Agreement for use with parents on receipt of these devices. As detailed in this Policy, safe use of online tools and resources is already integrated into the school curricula, with which the children receiving the devices are familiar.

The 1:1 devices will be secured with LGfL's HomeProtect Internet filtering solution. This will ensure that children using these devices from home receive the same level of filtering that they receive at school.

The Trust IT team will build on the work done during the periods of lockdown as a result of the Coronavirus pandemic to ensure that parents and children are provided with the necessary support. All arrangements will be subject to ongoing review to ensure that devices are used safely and appropriately. The Trust will manage any non-compliance with requirements as per usual procedures.

The Trust will also build on processes implemented and lessons learnt during the Coronavirus pandemic, during which devices were loaned to a number of families to ensure children had access to remote learning.

Given that, at this scale, this is a new provision, the IT Director will keep arrangements under close review.

2.20. Associated policies and explanatory documentation

- Child Protection and Safeguarding Policy

- ICT Acceptable Use Agreement and associated Policy
- Trust Privacy Notices
- IT Curriculum
- Online guidance for parents
- Trust Device Receipt Agreement (for parents)
- Trust Device Receipt Agreement (for staff)
- Cyber Security Policy
- Data Protection Policy
- Data Security Policy
- Records Retention Policy
- Data Protection Impact Assessments