South Lee Prep School
Bury St Edmunds

Acceptable Use Policy
September 2024

ISI Reference	12b
Key Author	DSL
Reviewed by	Head
Approval Body	Board of Governors
Approval Frequency	Annual
Last Approved	1st September 2024

Signed:	Steve Honeywood, Chair of Governors 1/09/24

Acceptable Use Policy (AUP)

Security

- User names and passwords supplied to access the School's ICT Systems must be kept secure at all times. Do not share them with any other user or try to use another user's password. You will be accountable for any use of the system undertaken in your user name. Staff should never give their logon details to a pupil.
- It is not permissible to use School access credentials on any device used by the general public, for example hotels, libraries or airports. It is also not permissible to allow any browser to save these credentials for easier use – staff must explicitly enter their user name and password each time they access the system and not record this information anywhere that others can discover it. Regular password changes will be implemented to augment this security.
- You must log off when you have finished using a computer or are leaving the room. If you are away from the room temporarily, then lock the computer.
- Shut down your computer and any whiteboard projector or screen at the end of each day.
- Do not try to disable or circumvent the School's anti-virus system, gain unauthorised access to any data or system which you do not have permission to use, or corrupt or destroy any other user's data or work.

GDPR & DATA PROTECTION – YOUR OBLIGATIONS

- **Ensure that personal data is kept fully secure at all times (computer and paper based). Do not send personal data to anyone not authorised to read it.**
- **Do not copy personal or confidential information from the system for use outside the school.**
- **Never use external devices, such as USB/memory sticks, external hard drives on the School's system. If you need to access data on the system from outside, use the share-point service to access the system.**
- **Keep your password secret.**
- **Always lock your computer screen when you step away, even if only for a few minutes.**
- **When freezing images on smart screens, use the FREEZE function, not the PAUSE function.**
- **The children's Action Plans must not be copied or printed. Action Plans may only be accessed and updated on the school network.**
- **If you need to share data with a new third party, check with the Business Manager that a Data Processing Agreement has been sent.**
- **Under Data Protection legislation, any information recorded about an individual may be the subject of a Subject Access Request, including opinions and intentions regarding that individual. For this reason, be careful about the data that you record and keep.**
- **Subject Access Requests must be referred to the Business Manager as soon as they are received – never send out personal data in response to a request yourself.**

- **Remain vigilant to potential Data Breaches at all times - it is your responsibility to notify the Business Manager <u>immediately</u> if you think a data breach may have taken place.**

Email

- Only the School's email system can be used for sending and receiving school related emails of a personal or confidential nature. **<u>Do not forward School emails to personal, non-School email accounts</u>.**
- Check the content of email messages before you send them to ensure that they may not be construed by recipients as harassment or abuse of any kind.
- Do not forward email containing information sent to you in confidence, or which a named person could reasonably regard as confidential.
- Do not use your School email address for any purpose that is not related to your School work.
- The content of communications will be monitored where necessary. Therefore, the content of your communications using the School's systems cannot be regarded as completely confidential.
- The purpose of monitoring is to ensure that the School's systems are used primarily to further the purposes of the School, that they are not used for inappropriate and/or unlawful purposes, and that system capacity is sufficient for the needs of the school.
- Incoming and outgoing mail is filtered for viruses and unacceptable attachments and may be filtered for unacceptable language. Spam may be blocked without any warning to sender or recipient.

Images

- Photographs of the children should ideally be recorded on the school digital devices. If you need to take pictures of the children eg on a fixture, trip or specific lesson you must send to the office and then delete the pictures/videos from your phone.
- Do not download images of the children onto your home computer or upload them to the internet unless to a system specifically designated by the school for that purpose.

Accessing ICT Systems Outside of School

- School systems can be accessed remotely through Office 365, with your standard log in.
- When using the Office, take extra care where other members of a household or family share a computer to ensure it is only signed in when the staff member is using the computer. A home computer used for any School work must be password protected and the password only known to the staff member concerned.
- If you use a School laptop/computer the Business Manager will record that you have it. You agree to be responsible for its care and security at all times. When travelling with any such equipment it must be taken as hand luggage and never left unattended. Laptops will be encrypted wherever possible.

Software

- Do not download any installable or executable software, or install any non-approved software onto any school PC (i.e. Spotify, Dropbox or similar). Do not load or run games CDs, music CDs, or connect any MP3 players, iPods, phones or similar devices into any school computer. If you do require something specific for your lessons/assembly please speak to the IT contractor to ensure it is safe to use.
- When proposing a new software provider or application, check with the Business Manager whether a Data Processing Agreement is in place with the proposed provider.
- The School has been granted licence agreements by software owners authorising the School to use their software. School software must not be installed on privately owned computers without permission from the Business Manager. To do so is highly likely to breach copyright or licence terms.

Safeguarding

- All reasonable steps must be taken to ensure that children are prevented from gaining access to confidential data stored on the network and unsupervised access to the Internet.
- When entering start-up or log on passwords, ensure that staff cannot be observed by the children.
- Remember that it is crucial to understand that a filter can reduce, but not eliminate the risk of exposure to inappropriate material on the internet. Teachers must actively monitor children by continuously circulating and discussing with the children what they are doing. Teachers are encouraged to open tabs and to ask to examine a child's history of internet activity.
- Ensure that when supervising pupils, they know the correct procedure for reporting any encounter with inappropriate words or pictures.
- Staff are responsible for doing their utmost to ensure that content accessed by the children is entirely appropriate for their age and for dealing appropriately when children have accessed content that is not.

Remote Teaching and Learning (In the unlikely event)

- All remote teaching must happen via the school's Teams system, whether it is the teacher or the pupil who is remotely accessing the content.
- All lessons must be delivered and received in a public area and with pupils within earshot of their supervising adult.
- No 1:1 video contact should occur between teachers and pupils, without the teacher first informing the parents.
- All parties must be made aware before any recording of remote content is made and such recordings must not be shared on any platform external to the school's systems.
- Any use of the Chat feature within Teams should be done using professional and appropriate language in a way that does not disrupt the smooth running of the lesson.
- When the school is open and children are in attendance, only those children who are required to be at home due to Covid restrictions are permitted to access lessons via Teams and that should be done through prior arrangement with the school office.

Web Browsing & Social Media

- The school uses systems to monitor and filter all internet access/use. The system records and restricts access to prohibited sites (including terrorist and extremist material) and enables the Designated Safeguarding Lead to monitor all online activity using the school's systems.
- Note that accessing certain inappropriate sites might well constitute a criminal offence and that web filtering systems are not infallible.
- Do not attempt to access or download materials which could not reasonably be made available to pupils under 13.
- Do not knowingly access, view, store, download or forward any illegal, inappropriate or in any way offensive material (e.g. chain emails, pornography, racist, sexist or otherwise discriminatory jokes, etc) under any circumstances.
- Do not post comments, references, information about the School, or any materials relating to the School or your work in the School on websites, social media, blogs chat systems or forums etc.
- If you have become involved with unsuitable material, inadvertently, you should notify the Designated Safeguarding Lead immediately.

Internet Contact with Pupils (excluding contact via the school's 'southlee.co.uk' domain)

- Staff must not exchange information or files with pupils, or establish any internet contact with pupils, via social media at any time, since to do so may facilitate other contacts between pupils and unknown adults outside their control.
- Staff must not exchange emails or text messages with current pupils. Communication should be via the 'southlee.co.uk' emails where appropriate.
- If a child raises any other issue, then staff should offer to see the child face to face under normal arrangements in school.
- Once pupils leave the School, but remain under 18, the same rules continue to apply with regard to social networking sites, but simple, direct email correspondence is acceptable. For pupils of all ages, however, staff should be aware that electronic communication is a potentially risky area and extreme care is needed to avoid being drawn into any inappropriate correspondence.
- Staff must not give out their personal phone numbers to parents or children, however in an emergency this might be given out. A mobile phone may be necessary on a trip, but in this case, the school mobile should be used ideally.

Personal Usage

- The School's ICT systems must only be used in connection with the duties for which the School employs you. However, limited use of email and internet facilities for personal purposes is permitted. Any such use must be in accordance with this policy and must not disrupt staff duties or involve access to excessive audio and video materials.
- Abuse or excessive use of the telephone system, email and/or internet will be dealt with through the disciplinary procedure.
- The School cannot support, maintain or otherwise assist with the maintenance of privately owned computer equipment. Personal computing problems must not be referred to School ICT staff as they are not permitted, or insured, to undertake such work. The only exception to this is where an issue is identified with the School's own software, where the fault lies with the School's software, rather than the individual's hardware or software.
- School ICT equipment including telephones may not be used for gambling.

- Do not open an internet-only bank or savings account, or other financial, shopping or trading account if the School provides your only route into this account. The School cannot guarantee to continue to provide access to such sites and cannot be responsible for any difficulties encountered.
- The School is concerned that space on its systems may be consumed unnecessarily if staff use the network to store personal files. Storage of digital photographs or digital video must be restricted to school use. Personal files found on the school system may be deleted without warning or notification.

General

- No food or liquids should be taken into any ICT space as it is both a bad example to the children and a risk of spillage and consequent shock.
- Printing is centrally monitored. Avoid unnecessary printing and where appropriate consider printing on both sides of a sheet of paper and using recycled paper. Please do not print in colour unless this is absolutely essential. Do not use the School's printing facilities for personal use.

Acceptable Use Policy Agreement

All staff and any governors, visitors who use the ICT equipment at South Lee School must sign to say that they will abide by this policy. See Appendix 1 below.
All Parents and Pupils will need to sign to say they abide by this policy through the form in Appendix 2

APPENDIX 1

ACCEPTABLE USE POLICY AGREEMENT – Staff, Governors and Visitors

Agreement

By signing below you confirm that you have read and accept the code of conduct for the use of **South Lee School's** ICT Systems as set out in the Acceptable Use Policy.

You agree to be bound by the contents from the date of signature, regardless of whether your engagement with the School has commenced at this date.

Name ____

Signed ______________________________ Date ____________

ACCEPTABLE USE POLICY AGREEMENT – Pupils

Agreement

By signing below you confirm that you have read, understood and agree to the rules of use of **South Lee School's** ICT Systems as set out in the Acceptable Use Policy, in conjunction with Digital Devices Guidelines for Parents and Pupils. If you do not sign and return this agreement, access will not be granted to the school ICT systems.

I have read and understood the Acceptable Use Policy and Digital Devices Guidelines for Parents and Pupils and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in school
- I use my own equipment out of school in a way that is related to me being a member of the school (communicating with other members of the school, using school email and Teams etc).

Name of Pupil ____

Class ____

Signed ____ Date ________________________

Parent/Carer Countersignature

Signed ____ Date ________________________