

LINSLADE LOWER SCHOOL

Information Technology Acceptable Use Policy

(e-Safety and e-Security)

Governor Approval:	January 2026
Review Cycle:	Annual (with safeguarding policy)

Policy review chronology:

January 2016	Esafety / Esecurity policies merged	Approved
January 2017	Additions made to 1.6.3 social networking. Social networking policy now merged to this policy.	Approved
January 2018	No additions but will need reviewing again when GDPR comes into force (May 2018) 1.6.3 Addition of Twitter account, also appendix 5 added	Approved
June 2018	Some minor amendments to reflect GDPR requirements. (Mostly in section 2)	Approved
January 2019	No additions	Approved
January 2020	No additions	Approved
January 2021	No additions	Approved
January 2022	No additions	Approved
January 2023	No additions	Approved
January 2024	Information related to KCSIE Sept 2023 included around filtering and monitoring Removed x (Twitter) policy	Approved
January 2025	Additional information about security of the internet- inline with Audit recommendations. RM Integris changes to RM Unify	Approved
January 2026	AI information added and references to old technology removed	Approved

LINSLADE LOWER SCHOOL

Information Technology Acceptable Use Policy

Introduction

It is the duty of schools to ensure that children and young people are protected from potential harm both within and beyond the school environment and to ensure the systems we use for administration and learning are secure and comply with data protection regulations.

Information & Communication Technology (ICT) in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access lifelong learning and employment. In addition, computer technology enables the school to carry out administration and management tasks efficiently and effectively.

ICT covers a wide range of resources, including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of ICT within our society as a whole. Currently, the information and communication technologies children are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality
- AI

The school has a comprehensive Safeguarding Policy in which a commitment to e-Safety is an essential element. This and the School's Data Protection & Information Security Strategy are designed to provide the necessary detail within that overarching policy.

There are two main elements to e-Safeguarding:

1. **e-Safety:** Procedures to ensure all members of the school community know their access rights and responsibilities in using ICT.
2. **e-Security:** Procedures to protect the physical network infrastructure to ensure all information and electronic data is securely maintained.

At Linslade Lower School the governors, school leaders and staff understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use (AU) Agreements (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile technologies provided by the school and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and portable media players, etc).

Section 1 E-Safety

1.1.0 Aims

1. To ensure the protection of all our children within and beyond the school setting by detailing appropriate and acceptable use of ICT-related technologies.
2. To outline the roles and responsibilities of everyone involved.
3. To ensure e-Safety is delivered as an integral part of the curriculum.
4. To ensure adults are clear about procedures for dealing with the misuse of any ICT-related technologies both within and beyond the school setting.
5. To develop links with parents/carers and the wider community to ensure their input into policies and procedures and continued awareness of benefits and potential issues of ICT-related technologies.

1.2.0 Risk assessment

- Both e-Security and e-Safety are based upon the assessment of risk and the implementation of controls to manage these risks. No use of ICT is completely risk-free.
- It is the responsibility of the Headteacher to ensure appropriate Risk Assessment procedures are in place.
- As a minimum, the risk assessment will be updated and reviewed by the Headteacher annually and reported to the Governing Body.

1.3.0 Roles and Responsibilities

1.3.1 The Governing Body

The Governing Body will:

- appoint a Governor with responsibility for e-Safety (this is included in the safeguarding governors' role).
- approve annually the Computer Acceptable Use Policy (this policy).
- receive periodic monitoring reports from the Headteacher regarding this policy.

1.3.2 E-Safety Governor

The e-Safety governor will:

- challenge the School about having a comprehensive and relevant AUP with appropriate strategies that define the roles, responsibilities for the management, implementation and safety in the use of ICT.
- ensure e-Safety is appropriately addressed as part of wider safeguarding within the school.

- challenge the School in its implementation and monitoring of relevant policies, procedures and practices.
- work closely with the member of staff who has responsibility for e-safety.

1.3.3 Headteacher

It is the overall responsibility of the Headteacher to ensure that there is an overview of e-Safety (as part of the wider remit of safeguarding) across the school, and s/he will specifically:

- Ensure relevant Risk Assessment procedures are in place and that these are updated and reviewed annually.
- Designate an e-Safety Leader to implement agreed policies, procedures, staff training, curriculum requirements, and take the lead responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment.
- Provide time and resources for the e-Safety Leader and staff to be trained and to update policies, where appropriate.
- Promote e-Safety across the curriculum and monitor its implementation in the classroom.
- Keep Governors informed about progress on the implementation of the e-Safety curriculum in relation to safeguarding.
- Ensure incident reporting procedures are in place and that any misuse or incident is dealt with appropriately.
- Periodically, the Headteacher will report to Governors any incidents that breach this and any other Safeguarding Policies.
- Appropriately monitor the implementation of this policy and periodically report to Governors.
- Review and update the AUP every year, incorporating any new legal requirements, recommendations from the LA and Central Government, and addressing issues arising from its implementation in preceding years.

1.3.4 E-Safety Leader

In this school, this is the subject leader for ICT.

It is the role of the Headteacher to:

- Support colleagues in how best to deliver the e-Safety message to pupils.
- Deliver training in new and emerging technologies relating to e-Safety.
- Work with the ICT technician to ensure internet filtering is set to the correct levels for staff and young people on the school network, on stand-alone PCs, laptops, etc. and the learning platform.
- Work with the ICT Curriculum Coordinator to ensure that there is appropriate and up-to-date anti-virus software and anti-spyware on the network, standalone PCs, laptops etc. and that this is reviewed and updated on a regular basis.
- Ensure that technicians carry out checks for viruses on laptops, standalone PCs, etc.

- Ensure that all staff and other appropriate adults are aware of the filtering levels and why they are there.
- Report issues to and update the Headteacher on an agreed regular basis.
- Keep a log of e-Safety incidents and analyse appropriately, allowing new and potential risks to be identified, thus helping to inform future development of safeguarding policies and procedures.
- These activities will be carried out in line with the most recent KCSIE.

1.3.5 Teachers & Teaching Support Assistants (TAs)

Teachers and TAs will actively:

- Teach children the safe use of ICT-related technologies.
- Encourage children to report any inappropriate materials or contacts straight away, without reprimand.

1.3.6 Staff and Other Adults (including the above-mentioned)

It is the responsibility of all staff and other appropriate adults to:

- Ensure that they know who the Designated Person is for Child Protection for the school so that any misuse or incidents involving a child can be reported and the correct procedures can be followed immediately.
- Report to the Headteacher immediately any inappropriate use of ICT-related technology by another member of staff or, in the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately
- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that in the event of misuse or an allegation, the correct procedures can be followed immediately. (In the event that a procedure is unknown, they will refer to the Headteacher).
- Alert the e-Safety Leader of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children are protected and supported in their use of online technologies so that they know how to use them in a safe and responsible manner and that they can be in control and know what to do in the event of an incident.
- Be up-to-date with e-Safety strategies in the classroom that are appropriate for the age group and reinforce them through the curriculum.
- Use ICT in a way that does not breach the Data Protection Act 1998.
- Keep in mind confidentiality and not to disclose information from the network, pass on security passwords or leave a station unattended when they are logged in.
- Ensure they have up-to-date anti-virus software and check for viruses on their work laptop (or personal laptop if used for work), memory stick or CD/DVD when transferring information from the Internet to the school network.
- Sign the relevant AU agreement.

1.3.7 Pupils

As relevant to their age and development, pupils will be expected:

- To use ICT resources in school for school purposes.
- To use a class email address or their own school email address (as appropriate to their age group) when emailing.
- To only open email attachments from people they know, or whom their teacher has approved.
- To keep their password secret and not to reveal it to others (except school staff).
- To only open/delete their own files.
- To know the rules for the safe use of the internet and sending/receiving emails. The children will understand what is expected of them with regard to behaviour and their attitude.
- The rules will be on display within the classrooms and in the computer suite, where this may be applicable.
- Not to use another pupil's workstation/computer without permission from a member of staff.
- To ensure that all ICT contact with other children and adults is responsible, polite and sensible.
- Not to deliberately look for, save or send anything that is inappropriate.
- To inform their teacher immediately if they find any inappropriate material on the internet.
- Not to give out their own details such as name, phone number or home address, and not to arrange to meet someone unless this is part of a school project approved by their teacher and a responsible adult accompanies them.
- To support the school approach to e-Safety and not deliberately upload or add any images, videos, sounds or text that could upset any member of the school community.
- To sign the relevant AU agreement.

1.3.8 Parents

The School believes that it is essential for parents/carers to be fully involved with promoting e-Safety both in and outside of school, and also to be aware of their responsibilities. The School regularly consults and discusses with parents/carers and seeks to promote a wide understanding of the benefits related to ICT and associated risks.

A leaflet will be sent home annually to all parents outlining Linslade Lower School's Acceptable Use Policy, and links to advice and guidance for the safe use of the internet will be provided.

Parents/carers will be:

- expected to explain and discuss the acceptable use and e-Safety rules with their child so that they are clearly understood and accepted.
- expected to sign the acceptable use agreement on behalf of their child on admission to school and return it to school, confirming both an understanding and acceptance of the rules. (The School will keep a record of the signed forms).
- required to make a decision as to whether they consent to images of their child being taken/ used in the public domain.

- encouraged to be involved with the monitoring of emails sent from and received at home.
- expected to sign the home school agreement containing the following statement -
“We will support the School’s approach to e-safety and the acceptable use of ICT and contact the school with any concerns regarding e-safety. We will ensure that our online activity will not cause the school, its staff, pupils or others distress or bring the school community into disrepute.”
- encouraged to contribute to adjustments or reviews of this policy by writing to the Headteacher.

1.4.0 Email

The use of email within the school is an essential means of communication for both staff and pupils. In the context of school and school-related business, email should not be considered private.

Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff-based or pupil-based, within school, national or international. The School recognises that children need to understand how to style an email in relation to their age and good network etiquette (‘netiquette’).

Managing Email

1.4.1 Staff

- The school gives all staff their own email account to use for all school business as a work based tool.
- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. The school email account must be the account that is used for all school business.
- Under no circumstances will staff contact pupils, parents, or conduct any school business using personal email addresses.
- All emails will be written and checked carefully before sending, in the same way as a letter written on school-headed paper.
- In the rare event that personal, sensitive, confidential or classified information needs to be transmitted via email, the consent of the Headteacher must be obtained. A secure portal is available for communication with Central Bedfordshire Council, and encrypted emails may also be sent to partner organisations.
- Emails created or received as part of school business will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.
- The forwarding of chain emails is not permitted.
- Staff must check their school email daily during term time (working days).
- The sending of inappropriate email messages between any members of the school community is not allowed.
- Staff must inform the school e-Safety Leader or their line manager if they, or one of their pupils, receives an offensive email.
- Within the classroom, teachers will introduce email to pupils as part of the curriculum and

to monitor their class use of emails.

- Regardless of how staff access their school email (whether directly, through webmail when away from school), all the school email policies apply.
- Never open attachments from an untrusted source; Consult the network manager first.

1.4.2 Pupils

- Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Key Stage 2 children will be given their own individual school-issued accounts; all other children will use a class/group email address.
- All pupil email users are expected to adhere to the generally accepted rules of netiquette, particularly in relation to the use of appropriate language and not to reveal any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission from an appropriate adult.
- Children are to use their school-issued email addresses for communication between home and school only.
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive email.
- However, pupils access their school email (whether directly, through webmail when away from school), all the school email policies apply.

Managing Mobile devices and digital images

1.5.0 Mobile Phones & Other Portable Devices, including iPads, laptops, smart watches

- The school allows staff to bring in personal mobile phones and devices for their own use. However, staff use of personal mobile telephones is permitted only outside lesson times and never in the presence of children. Personal calls/texts can be made or received in the staffroom. If privacy is required, please ask the Headteacher for the use of a private space. Mobile phones must be kept out of sight during the school day.
- Under no circumstances will the school allow a member of staff to contact a pupil or parent/carer using their personal device.
- Staff bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Pupils are not allowed to bring mobile telephones to school under any circumstances.
- The school has a mobile phone for use on school trips and off-site activities. Parents are not permitted to use mobile phones when assisting on school trips or visits.

1.5.1 Taking, Use and Storage of Pupil & Staff Images

Digital images are easy to capture, reproduce and publish and are therefore easily subject to misuse.

- With the appropriate permission, the school permits the taking of images (photographs or video) of staff and pupils with school equipment for educational purposes.
- The publishing of images of staff and pupils via the school website or for publicity purposes will require the appropriate permission.
- Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will also not be published.
- Staff and pupils are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils (this includes when on field trips).
- Parents are permitted to take images of their children at school events, but may not publish them in any form if they include those of other pupils or staff.

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos (including moving images) in the following ways:

- on the school website
- In the school prospectus and other printed publications that the school may produce for promotional purposes.
- In display material that may be used in the School's communal areas.
- In display material that may be used in external areas, e.g. exhibition promoting the School.
- General media appearances, e.g. local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

Explicit consent for each of these purposes is required. Consent will be sought on entry to school, but Parents/ carers may withdraw permission by writing to the headteacher at any time.

Written permission to use images of staff who work at the school will be sought on induction, and a copy of their consent form will be kept in their personnel file. The consent form will be considered valid for the entire period that the staff member is employed at the school unless they request to amend it.

1.5.2 Storage of Images

- Images/video films of children will be stored on the School's network.
- Pupils and staff will not be permitted to use personal portable media (e.g. memory sticks) for storage of images.
- Rights of access to this material will be restricted to the teaching staff and pupils within the confines of the school network.

1.5.3 Webcams

- The School will only use publicly accessible webcams as a teaching tool, and pupils will be strictly supervised.
- Webcams in school will be used for specific learning purposes (e.g. monitoring birds' nests) and never be used to capture images of children.

The Internet, social media and school website

1.6.0 Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material that makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

The Wi-Fi internet is password-protected. There is a password for guests with their own devices and another one for school staff.

1.6.1 Managing the Internet

- Pupils will only have supervised access to Internet resources through the School's fixed and mobile internet technologies.
- Staff will preview any recommended websites before use.
- Raw image searches will be discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. Parents will be advised to supervise this work and any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- School internet access will be controlled at two levels - through the LA's web filtering service and locally, where the LA filtering policy can be amended.
- Pupils and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the ICT coordinator.
- These activities will be carried out in line with the recent KCSIE.

1.6.2 Internet use

The School teaches how to use the Internet safely and responsibly, for researching information, exploring concepts, deepening knowledge, understanding, and communicating effectively in order to further learning.

Pupils will be taught the dangers of uploading or emailing personal information, which is high risk, and that it should not include:

- Full name (first name is acceptable, without a photograph)
- Address
- Mobile/home telephone number
- Email address
- School name
- Clubs attended and where
- Age or DOB
- Names of parents
- Routes to and from school

- Personal image
- Any other identifying information.

Staff should:

- only use the internet for personal use outside of lesson times.
- never gamble or game online in school.
- not purchase goods using School computers.
- not reveal names of colleagues or any other confidential information acquired through their job on any social networking site or blog.

1.6.3 Social Networking

Social networking includes activities such as:

- Blogging (writing personal journals to publicly accessible internet pages),
- Social networking sites such as Facebook
- The posting of material, images or comments on websites such as YouTube
- Online discussion forums
- Collaborative spaces
- Media sharing
- Microblogging applications such as Twitter
- MSN
- Virtual worlds
- WhatsApp
- Snapchat

This list is not exhaustive.

Social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, the School recognises that there are issues regarding the appropriateness of some content, contact, culture and commercialism and some potential dangers.

The potential dangers inherent in these activities include:

- Potential negative effect on an organisation's reputation or image.
- Compromising the schools commitment to safeguarding children.
- Breaching school confidentiality procedures.
- Staff grievances leading to disciplinary cases.
- School leaders and governors are exposed to legal risks.

Pupil use:

To this end, the School encourages pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- The school will endeavour to deny access to social networking sites to pupils within school, but recognising that many will have access at home. All pupils will be advised to be cautious about the information given by others on sites.

- Pupils will be taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils will be reminded to avoid giving out personal details (see above) on such sites that may identify them or where they are.
- Pupils will be advised to set and maintain profiles on such sites to maximise privacy and deny access to unknown individuals.
- Pupils will be encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils and parents will be asked to report any incidents of bullying via such sites to the school.

Staff use:

- All staff have a responsibility to ensure that they protect the reputation of the school, and treat colleagues and members of the school community with professionalism and respect.
- It is important to protect all staff and members of our community from allegations and misinterpretations which can arise from the use of social networking sites.
- Safeguarding children is a key responsibility of all members of staff, and it is essential that staff act responsibly if they are using social networking sites out of school.
- Anyone working in the school, either as a paid employee or volunteer, must not communicate with children via social networking.
- Accessing social networking sites at work using school equipment is not permitted.
- The use of the school's name, logo, or any other published material without written prior permission from the Headteacher is not permitted.
- No communications, irrespective of their anonymity, should be shared that relate to any specific event, protocol, pupil or person at School.
- All information shared through social networking applications, even via private spaces, is subject to copyright, data protection and Freedom of Information legislation & the Safeguarding Vulnerable Groups Act 2006.
- School staff must not invite, accept or engage in communications with parents or children from the school community on any personal social networking sites.
- Any communication received from children (past or present) to School Representatives must be immediately reported to the Head Teacher – Designated Child Protection Officer, and procedures for safeguarding followed.

- If a School Representative is made aware of any other inappropriate communications involving any child and social networking, these must be reported immediately as above.

1.6.4

The School Website and APP

The School website is maintained by the school.

- The uploading of images to the school website will be subject to the same acceptable use rules as outlined above.
- The Headteacher will consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

Teaching and learning

1.7.0 E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. The School believes it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis. e-Safety will be embedded within the curriculum, and teachers will continually look for new opportunities to promote e-Safety.

- e-Safety will be introduced to the pupils at the start of each school year.
- The school has a framework for teaching e-safety that is linked to the units of work in the computing curriculum.
- Opportunities to consolidate e-Safety skills are provided whenever ICT is used.
- Educating pupils on the dangers of technologies that may be encountered outside school will be done informally when opportunities arise and as part of the e-Safety curriculum.
- At an appropriate age, pupils will be made aware of the relevant legislation when using the internet, such as data protection and intellectual property, which may limit what they want to do but also serve to protect them.
- Pupils will be taught about copyright and respecting other people's information, images, etc., through discussion, modeling and activities.
- Pupils will be made aware of the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils will also be told where to seek advice or help if they experience problems when using the internet and related technologies, e.g. parent/carer, teacher/trusted staff member, or organisations such as Childline and CEOP report abuse button.
- Pupils will be taught to critically evaluate materials and learn good searching skills through discussions and via the curriculum.
- e-Safety posters will be prominently displayed in classrooms and around the school.

1.7.1 E-Safety Skills Development for Staff

- School staff will receive regular information and training on e-Safety issues.

- A record of relevant training will be kept.
- New staff will receive information on the school's acceptable use policy as part of their induction.
- e-Safety in the wider context of the protection of children and know what to do in the event of misuse of technology by any member of the school community.

1.7.2 Pupils with Additional Needs

The school will endeavour to create a consistent message with parents for all pupils, and this, in turn, should aid the establishment and future development of the school's rules.

However, the School is aware that some pupils may require additional teaching, including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration will be given to group interactions when raising awareness of e-Safety. Internet activities will be planned and well-managed for these children.

Section 2 E-Security

2.1.0 Data protection and data security strategy

At Linslade Lower School, the governors, management and staff understand their responsibility to protect data on pupils and staff that, if allowed to be accessed by others, could lead to a breach of the General Data Protection Regulation and a consequent risk to the safety of individuals.

The School Data Protection & Information Security strategy is based on the premise that information should flow as freely as possible, but that access to information should be permitted on the basis of "need to restrict" rather than "need to know". This strategy does not conflict with the need to protect sensitive information and to safeguard the accuracy and completeness of information and computer software.

2.1.1 General Data Protection Regulation (GDPR):

The General Data Protection Regulation (GDPR) imposes statutory conditions for the maintenance of personal data on school computer systems, including data held by individual members of staff on PCs. It is an offence to use or disclose such data if not registered to do so. Staff may use or store data on individual pupils on their school-issued laptop.

Data Protection Principles:

Personal data must be processed (gathered, shared, manipulated, stored and destroyed) in accordance with these principles:

- It must be processed lawfully, fairly and transparently.
- It must be processed for a purpose that has been explained to the data subject.
- Only data that is adequate, relevant, and limited to the data needed for the specified process can be processed.
- Data processed must be accurate and, as far as possible, up to date.

- Data must be kept for no longer than is necessary for the performance of the specified purpose.
- Data must be kept secure
- Data will be disposed of in a secure manner

The school has to demonstrate compliance with these principles.

2.2.0 Computer Viruses

- All networked school computers will have anti-virus software installed that is automatically updated (minimum daily).
- This anti-virus software will automatically check all files downloaded from the Internet, received via e-mail or on removable media (e.g. memory stick). Staff must respond to any warning messages appropriately.
- Staff and pupils must never interfere with any anti-virus software installed on school ICT equipment.
- Staff using a laptop that is not routinely connected to the school network or their own laptop must make provision for regular virus updates through the ICT coordinator.
- Staff preparing schoolwork on their home computers, and using portable storage media, are expected to maintain effective and up-to-date anti-virus protection on their machines.
- Staff who suspect there may be a virus on any school ICT equipment must stop using the equipment and contact the ICT coordinator immediately, who will advise what actions to take.

2.3.0 Passwords and Password Security

Password security is essential for staff, particularly for those who are able to access and use pupil data. Staff will have secure passwords that are not shared with anyone. The pupils are expected to keep their passwords secret and not to share them with others, particularly their friends. Staff and pupils will be regularly reminded of the need for password security.

- Staff and pupils are provided with an individual network and Management Information System (where appropriate) log-in usernames and passwords.
- Staff and pupils (where applicable) will always be expected to use their own personal usernames and passwords to access computer-based services.
- Staff must change their password whenever there is any indication of possible password compromise. Pupils must inform their teacher, who will arrange for their password to be changed.
- Pupils are not allowed to deliberately access online materials or files on the school network, of their peers, teachers or others.
- Staff will be regularly reminded of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems, including ensuring that passwords are not shared and are changed periodically.
- Staff must not record passwords or encryption keys on paper or in an unprotected file.
- Passwords for the Management Information System must contain a minimum of six characters and be difficult to guess.

- User IDs and passwords for staff and pupils who have left the School will be removed from the system in a timely manner.
- Individual staff users must also make sure that workstations logged onto the network are not left unattended – unless password-locked.
- Terminals that can be logged on to the School's MIS database must have an automatic screen lock after being left unused for 3 minutes.
- All access to the School's MIS database must be subject to account locking after a maximum of 5 failed login attempts.

2.4.0 Remote Access

Potentially, school staff can remotely access their school emails, and a few named individuals have the authority to access the School's RM Unify system, containing pupil and staff data, through the internet from home.

The following guidelines apply when accessing the RM Unify system and information away from the school:

- All user remote access will require a username and password.
- Computers/workstations used to access the system will be regularly patched with the latest security updates, have an anti-virus system that is updated every time the computer is switched on, and have firewall software activated.
- All remote access should be subject to account locking after a maximum of 5 failed attempts.
- No data from the system will be stored on the workstation's hard disk or portable media.
- The computer/workstation will lock if not used for five minutes; unlocking will require the user's password.
- Access to data remotely will be part of the wider risk assessment of data security.
- Users will protect School information and data at all times, including any printed material produced while using the remote access facility.
- Users will be particularly careful not to allow any family members access to data/information.

2.5.0 Data Backup & Storage

- Pupil and staff sensitive information must not be stored on any mobile devices unless encrypted.
- Backup of staff and pupil data in the online management information system is automatic and provided by the management company under contract.
- Backup of the School's financial data must be backed up at least twice weekly or after a large number of amendments have been made. A monthly backup copy must be kept off-site.

2.5.1 Continuity Planning

- All school information systems are subject to potential loss of data due to failure of software or hardware media. It is the responsibility of the Headteacher to ensure that regular back-up copies of essential data on the network servers are made and stored in a safe location, remote from the system

-

2.5.2 Disaster Recovery

There is a risk that an entire system may be lost as a result of a disaster, e.g. fire or flood. For central systems where an alternative system platform and software may not be readily available, then other provision will be made on the basis of a risk assessment analysis by the Headteacher.

Section 3 Management of incidents

3.1.0 Incident Reporting

It is the responsibility of the Headteacher to ensure incident-reporting procedures are in place and implemented. Periodically, the Headteacher will report to Governors any incidents that breach this and any other Safeguarding Policies.

An important element of e-Safety / e-Security is the ability to identify and deal with relevant incidents. All staff and pupils have a responsibility to report e-Safety or e-Security incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact on the school and individuals.

The Headteacher will establish an incident reporting procedure and record reported incidents in an Incident Log. This log should capture the following information:

- Incident date
- Description of the occurrence
- Immediate corrective action
- Further action
- Legal implications
- Incident closure date

The Incident Log will be formally reviewed, and any outstanding actions delegated, by the Headteacher at a minimum frequency of once per term. Through this review process, where deemed appropriate, management will update the risk assessment in light of new incidents.

3.1.1 Monitoring

Authorised school staff may inspect any ICT equipment owned or leased by the School at any time without prior notice.

Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business-related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the General Data Protection Regulation, or to prevent or detect crime.

Authorised staff may, without prior notice, access the email or voice-mail account, of someone who is absent in order to deal with any business-related issues retained on that account.

- All monitoring, surveillance or investigative activities are conducted by authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000. These activities will be carried out in line with the recent KCSIE.

Personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

3.1.2 Breaches of Policy

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, this policy outlines the correct procedures for ensuring staff achieve acceptable standards of behaviour and comply with the rules of the Governing Body.

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or other ICT services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedures. Policy breaches may also lead to criminal or civil proceedings.

3.1.3 Review Procedure

- There will be an ongoing opportunity for staff to discuss with the e-Safety Leader any issue of e-Safety that concerns them.
- This policy will be reviewed annually and consideration given to the implications for future whole school development planning regarding child protection.
- The policy will be amended if new technologies are adopted or the Central Government change the orders or guidance in any way.

Section 4 Policy dissemination and review

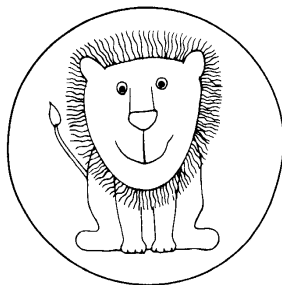
4.1.0 Policy Distribution

- All staff will receive a copy of this policy on recruitment to the school or at any time the policy is amended.
- All governors will receive a copy of this policy as part of their induction.
- A copy will be available on the school website.

4.1.1 Policy review

The governors will review this policy every year at the same time as the safeguarding policy.

Appendix 1

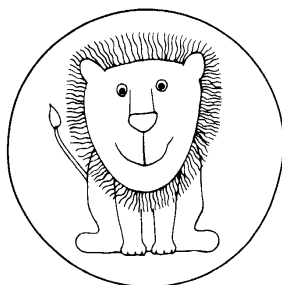


Linslade Lower School Acceptable use of Information Communication Technology Reception Pupil Agreement

Agreement / eSafety Rules

- I will only use ICT in school when my teacher says I can
- I will only use ICT in school to do the activity my teacher has told me to



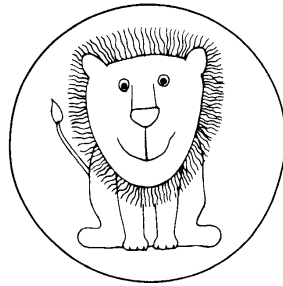


Linslade Lower School
Acceptable use of Information Communication Technology
Key Stage 1 Pupil Agreement

Agreement / eSafety Rules

- I will only use ICT in school when my teacher says I can
- I will only use ICT in school to do the activity my teacher has told me to
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- If I accidentally find anything unpleasant or nasty I will tell my teacher immediately.
- I know that my use of ICT can be checked and my parent will be contacted if a member of school staff is concerned about my safety.
- I will not bring a mobile phone to school because I am not allowed to.





Linslade Lower School
Acceptable use of Information Communication Technology
Key Stage 2 Pupil Agreement

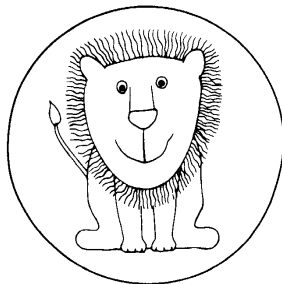
I Agreement / eSafety Rules

- I will only use ICT in school for school purposes
- I will only use my class e-mail address or my own school e-mail address when e-mailing
- I will only open e-mail attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carers contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a

school project approved by my teacher

- I will not bring a mobile phone to school because I am not allowed to
- I will not sign up to online services until I am old enough.

Appendix 4



Linslade Lower School Staff, Governor and Visitor Acceptable Use Agreement

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on RM integris) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature Date

Full Name(printed)

Job title

