LINCOLN GARDENS PRIMARY SCHOOL

ESAFEGUARDING POLICY

PERSON RESPONSIBLE FOR POLICY:	**RYAN SMITH**
APPROVED: GOVERNING BODY	**DATE: NOVEMBER 2020**
SIGNED:	**ROLE:**
TO BE REVIEWED:	**SEPTEMBER 2021**

LINCOLN GARDENS PRIMARY SCHOOL
e-safeguarding POLICY

Policy Focus

Lincoln Gardens Primary School is committed to realising the benefits of ICT as a valuable learning resource for every pupil and member of staff. ICT also provides the school with effective means of data protection compliance whilst ensuring an efficient business function and communication channels across the school and wider community. However, in doing so, the school is cognisant of the risks involved in providing whole school ICT technologies and this policy is designed to ensure all users are equipped with sufficient knowledge of e-safeguarding procedures to protect themselves and the school as a whole. First and foremost, learning is central to the school's ideals and values in determining appropriate and effective ICT resources. We will endeavour at all times to embrace technological advancements where doing so complements and supports learning in preparing children for the future. ICT technologies are accepted as an integral part of the whole school community. The purpose of Lincoln Garden's e-safeguarding policy is to ensure access to these resources is provided, as far as reasonably possible, in a safe and well informed environment, adjusted to the age, ability and specific needs of each child. Staff and governors accept that the internet provides a wealth of additional learning opportunities, which, if used appropriately and responsibly, will enhance and integrate with existing curriculum tools.

This policy should be read in conjunction with the school's Acceptable Use Policy.

It is important to accept that the pace of change within technological developments may require this policy to be reviewed at regular intervals. However, the main focus of this policy is to equip stakeholders with sufficient knowledge and guidance to make informed and responsible decisions to protect the individual and the school community as a whole, whilst promoting an effective and creative online learning environment. The aims of this policy are summarised as follows:

- To promote and maintain a safe, positive and innovative environment for learning from the perspective of both staff and pupils.
- Create a culture of pupil led learning related to esafety and appropriate use of technologies.
- To provide the whole school community with an understanding of the risks associated with on-line activity both at school and at home.
- To ensure staff and pupils understand the principles of 'whistle blowing' and are confident to use this when necessary.
- To embed the principles of the school's e-safeguarding policy framework within day to day activities to provide an effective means of protecting all users.
- To engender a balance between optimising the benefits of known and emerging ICT technologies with effective risk management techniques.
- To provide clear and concise guidance as to the required procedures and control measures in place to facilitate a safe learning environment.
- To provide clear and concise guidance as to the required procedures and control measures in place for the effective management of school data and information which are compliant with the Data Protection Act.

There is a separate policy in place for pupils; differentiated according to Key Stage.

For this policy to be effective it will be assumed a responsibility of all governors and staff to ensure the principles and scope of the policy are integral to all school based activities and those which are deemed to be linked to the school community by association. The Lincoln Gardens e-safeguarding Policy forms part of the induction process for all new staff and governors. A summarised version will be provided to:-

- those working within school on a temporary basis in the capacity of short-term paid employment,
- individuals undertaking voluntary work,
- students on work experience placements,
- visiting members of staff.

- External agencies

Scope of the Policy

The use of web based and other ICT technologies has increased significantly over recent years and it is incumbent upon the school to assess the viability and appropriate use within an educational setting. The pace of change is rapid and it is therefore necessary to have in place a framework to ensure members of the school community have sufficient information and guidance in order to make informed decisions about the development and management of ICT in school. With this in mind, the Lincoln Gardens e-safeguarding policy sets out to provide a comprehensive framework to protect the interests of all stakeholders whilst facilitating a rich and dynamic learning environment. As far as reasonably possible, the school will endeavour to achieve a balance between innovation in its strategic vision to ensure new and emerging technologies are embraced, whilst adhering to e-safeguarding practices. In this way all stakeholders will benefit from:-

- Provision of a clear code of practice for the use of all technologies in school.
- Provision of a clear code of practice for the use of mobile technologies as well as accessing school based information remotely.
- Setting out standards of behaviour and acceptable use of ICT resources for learning, business and social use.
- Protecting the reputation of individuals and the school against mis-representation, malicious or false allegations.
- Provision of an effective means of monitoring and reviewing compliance with this policy.
- Ensuring compliance with the school's responsibilities under the Data Protection Act; understanding our responsibilities as Data Controller and Data Processor.
- Ensuring we are aware of our responsibilities relating to the Freedom of Information Act.
- Providing an effective means of recording incidents which threaten or potentially threaten to breach the terms and conditions of the Lincoln Gardens Primary School's e-safeguarding and acceptable use policies. Where appropriate this will include reporting procedures to the relevant authority and reference to the school's disciplinary procedures where sanctions are deemed necessary:-
    - Incidents and potential e-safeguarding problems relating to pupils and general issues will be recorded electronically in the incident log located in the leadership drive.
    - Incidents relating to staff, governors and pupils (where there are known or new child protection issues) will be recorded electronically in the leadership drive.
    - Both logs will be monitored and reviewed by the e-safeguarding committee to ensure the school is acting with due regard to the principles of this policy in protecting members of the school community.
    - Notwithstanding the above, the school's whistleblowing policy will be implemented where any member of the school community has serious and immediate concerns for the safety, welfare and protection of any other individual.
    - Whistleblowing procedures will also be followed where any individual has serious and immediate concerns relating to the wilful and deliberate mis-use or manipulation of the school's IT resources (both hardware and software) which is likely to pose a threat to the school community as a whole. This might include:-
        - Deliberate physical damage to equipment
        - Deliberate acts in contravention of any aspect of the school's acceptable use policy
        - Alteration or manipulation of any personal data relating to pupils and staff without the express permission of the subject.
        - Alteration or manipulation of school based performance, achievement or target related data.

Communication and review of policy

Lincoln Gardens Primary e-safeguarding policy will be included within the school's induction pack for all new members of staff and governors. Policy revisions and updates will be communicated to all staff and governors by email alert, indicating the location of the updated electronic document. (In the case of governors, a revised copy with be attached to the email). Members of staff without access to the school's email system will be

provided with a paper copy. A file containing a copy of all school policies will be available in the staff room and on the school's website.

This policy will be reviewed annually. However, amendments to the current policy may be deemed necessary when:-

- A review of the incident logs indicates a change in policy wording is required
- Changes in the school's ICT infrastructure, use of software and/or media, necessitates review
- A new threat to security or safeguarding has been identified
- Changes in legislation and/or guidance by government agencies
- Advancements in technology need to be incorporated as additional safeguarding measures

Any changes to the school's e-safeguarding policy will be discussed by the leadership team and ICT Co-ordinator to ensure changes are consistent within the context of the school's ICT framework.

Key Personnel

Designated Safeguarding Lead	Headteacher, Miss Andrea Nuttall
Deputy Designated Safeguarding Lead	Deputy Headteacher, Mr C Jackson
Governor responsible for safeguarding	Mr Alan Smith
Data Protection Officer	Business Manager, Mrs Claire Mallia
E-Safety Lead	Mr Ryan Smith
ICT Technician	Mr Matthew White

Governors

Governors have ultimate responsibility for approving and adopting all policies and in monitoring their effectiveness:-

- To review and approve the school's e-safeguarding policies, ensuring that all governors understand policy content and actively promote e-safeguarding awareness.
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils
- To develop an overview of how the school ICT infrastructure provides safe access to the internet
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school
- To support the work of the e-safeguarding committee in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in e-safeguarding activities
- To ensure appropriate funding and resources are available for the school to implement its e-safeguarding strategy
- Day to day responsibility is delegated to the Headteacher and leadership team.

Headteacher and senior leadership team

- The headteacher is responsible for all safeguarding provision (including e-safeguarding) as part of the school's security, safeguarding and child protection suite of policies within school. However, day to day management is delegated to the e-safeguarding co-ordinator.
- The Headteacher, together with the Leadership team will take any action required as a result of monitoring reports submitted by the e-safeguarding co-ordinator.
- The Headteacher and leadership team are responsible for taking action in the event of any security breach or other critical incident.
- As Designated Safeguarding Lead, the Headteacher, supported by the senior leadership team, will ensure:-
    - Pupils and their families are provided with relevant and timely support relating to e-safeguarding issues which are relevant to their current situation
    - Confidential and/or sensitive pupil information remains confidential and is only shared with those who have a legitimate and justifiable reason for access.

    - That children and, when appropriate their families, understand the dangers regarding access to inappropriate online contact with adults and strangers
    - That all staff are aware of the potential for on-line grooming of young children
    - That all staff understand the implications of cyberbullying and the use of social media for this purpose.
- The headteacher will ensure that relevant e-safeguarding training is and senior leadership team are responsible for ensuring that the e-safeguarding Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safeguarding roles and to train other colleagues when necessary.
- The headteacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious e-safeguarding incident.
- The headteacher and senior leadership team will receive update reports from the incident management team

E-safety lead

- To promote an awareness and commitment to e-safeguarding throughout the school community
- To take day-to-day responsibility for e-safeguarding within school and to have a leading role in establishing and reviewing the school e-safeguarding policies and procedures
- To have regular contact with other e-safeguarding committees, e.g. the local authority, Local Safeguarding Children Board
- The E-Safety Lead will have regular contact with the leadership team, governor responsible for e-safeguarding and ICT Technician
- To ensure robust e-safeguarding policies and procedures are in place which are communicated to all staff and pupils through regular training and updates
- To ensure that e-safeguarding education is embedded across the curriculum
- To ensure that e-safeguarding is promoted to parents and carers
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate
- To monitor and report on e-safeguarding issues to the e-safeguarding group and the senior leadership team as appropriate

Vulnerable Child Group meetings

- To review incident logs and report their findings to the senior leadership team
- To use knowledge acquired through regular review and appraisal of school procedures and incident logs to inform changes in policy.
- To ensure that school Acceptable Use Policies are appropriate for the intended audience
- To promote to all members of the school community the safe use of the internet and any technologies deployed within school

All staff

- To read, understand and comply with the school's e-safeguarding policies and guidance.
- All staff will read, understand, sign and comply with the school's Acceptable Use Policy (AUP).
- All staff have an obligation to report any incident relating to unsafe practices, mis-use of equipment or breach of policy. (Whistleblowing Policy)
- All staff will attend relevant e-safeguarding training and updates when required. Individual members of staff who have missed training due to absence will alert their line manager to ensure any missed training is received.
- All staff have a responsibility to follow e-safeguarding procedures and seek advice from key personnel when necessary to clarify their understanding and ensure they are fully compliant with school policy.
- All staff should demonstrate high levels of professional conduct at all times.
- All staff will promote and model appropriate e-safeguarding procedures across the school community, ensuring such practices are embedded within all curriculum and extra-curricular activities

Technical staff

- To read, understand, contribute to and help promote the school's e-safeguarding policies and guidance
- To read, understand, sign and comply with the school's Acceptable Use Policy.
- To support the Headteacher and leadership team in monitoring compliance with the Acceptable Use Policy.
- To act as a contact for pupils' whistleblowing procedures.
- To report any e-safeguarding related issues to the e-safeguarding coordinator or SIRO.
- To maintain a high level of professional conduct at all times, in particular being aware of own enhanced levels of technical expertise and access privileges necessary to effectively discharge duties within this role.
- To be responsible for the maintenance and development of the school's ICT network and infrastructure, consistent with the aims of the school's e-safeguarding policy and development plan.
- To ensure there are adequate measures in place for back up of school data and retrieval of data in the event of a critical incident (Business Continuity Plan)
- To ensure, as far as reasonably possible, that the school network and infrastructure is protected from malicious attack.
- To report any breach of security to the senior leadership team.
- To ensure there are robust procedures in place for:-
    - Access and log-in
    - Differentiated levels of access appropriate to role
    - Protecting administrator rights
    - Maintaining an inventory of all hardware and software
- To develop and maintain a good understanding of current e-safeguarding issues including data protection.
- To be a member of the e-safeguarding committee and contribute to decision making processes concerning e-safeguarding procedures.
- To liaise with the local authority and YHGfL on technical issues, best practice and opportunities to advance skills and knowledge.
- To provide training for all staff, relevant to their role, at appropriate intervals, as required by the Headteacher and leadership team.
- To document all technical procedures and review them for accuracy at appropriate intervals
- To investigate proposed online services to ensure they comply with the school's data protection and safeguarding policies

Teaching & Learning

- We will provide a series of specific e-safeguarding-related lessons in every year group/specific year groups as part of the Computing curriculum / PSHE curriculum / other lessons.
- We will celebrate and promote e-safeguarding through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant e-safeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an end-user Acceptable Use Policy which every pupil will sign/will be displayed throughout the school/will be displayed when a pupil logs on to the school network.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, safe search is implemented by default through the proxy. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- All pupils will be taught in an age-appropriate context about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.

- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button

Use of third party resources

The school accepts that curriculum activities will include the use of third party resources to enrich elearning experiences, develop enhanced communication channels between pupils and provide opportunities for interaction beyond the school community. For example:-

- Sharing work through social media
- Sharing of good practice
- Networking and developing ideas
- Email
- Online storage services (Onedrive etc)

Prior to establishing links with any third party or entering into an agreement for the provision of services to deliver any of the above, the school (SIRO and ICT Technician) will carry out a risk assessment to determine if the provider has adequate provision in place for the following:-

- Data Protection/Security Policy
- Statement relating to the retention of data, backups, transmission to any other party (this may be included within the Data Protection/Security Policy to enable to school to establish what happens to pupil and/or staff data on completion of the agreement or project period.
- Location of back-up files. We will ensure that the provider uses EU compliant storage facilities and in all respects complies with the Data Protection Act.
- Declaration relating to the ownership of data files. It is important that the school retains ownership of data relating to any member of the school community taking into account its responsibilities under the Data Protection Act.
- We will ensure that any third party provider is registered as a Data Controller.
- Where pupils have contact either directly or indirectly with staff employed by third party providers, we will ensure that the provider has put in place adequate safer recruitment measures to safeguard the interests of all pupils and staff who may interact with them.

Staff training

The school is committed to ensuring e-safeguarding training is delivered to all members of the school community so that they become confident users of IT appropriate to their role, equipped with the necessary knowledge and awareness of the risks associated with the use of ICT.

- New members of staff will be provided with a copy of the school's e-safeguarding policy as part of their induction programme as well as a meeting with the e-safety lead
- They will be expected to comply with the terms of the school's Acceptable Use Policy by signing and returning one copy of the agreement.
- Training will be delivered as a priority to new members of staff, prior to being provided with access to the internet and school network.
- Refresher training will be delivered at appropriate intervals to keep staff well informed of changes in legislation and when developments in technology dictate a change in policy wording. (Communication and Review)
- Members of staff with particular whole school responsibilities (e-safeguarding, child protection, data security, ICT and network management) will also discuss the school's ICT strategy and measures required to address objectives within the School Development Plan through:-
    - Planned meetings
    - Informal discussion
    - Networking opportunities with other schools and organisations

- Minor changes to policy wording will be communicated via email. Staff will be expected to confirm by acknowledgement of a 'read receipt'.
- All staff will endeavour to incorporate the principles of effective e-safeguarding practices across all elements of their employment at Lincoln Gardens Primary School.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-safeguarding and know what to do in the event of misuse of technology by any member of the school community.

Managing ICT systems and access

- The school will employ a suitably qualified and experienced ICT Technician who will take responsibility for the management, monitoring and updating of all IT equipment and IT infrastructure. The remit of the ICT technician will include sufficient responsibility and level of expertise consistent with the effective management of all ICT systems, overseen by the Strategic Data Lead
- The school will establish links with the local authority's business support services and YHGfL to ensure staff have access to specialist training, promotional activities and workshops etc.
- Access to school systems will be assessed and allocated on a need to know basis. Similarly, access to the internet will be monitored and assigned at level appropriate to the user.
- All school network servers and other key hardware will be sited within the communications room; a lockable internal store room. Allocation of keys will be restricted.
- All users will sign an end-user Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.
- Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. They will abide by the school AUP at all times.

Passwords

The school follows guidance issued by the ICO (Information Commissioner's Office) in ensuring staff adhere to a robust password policy. The policy exists to ensure the school discharges its duties responsibly with regard to the Data Protection Act and applies to all log-in procedures required for network access, email and information management systems.

Following induction, new users will be issued with a user name and initial password. Users are required to change their password to one which complies with the password policy:-

- Not contain part of your username or full name that exceeds two consecutive characters
- Be at least eight characters in length
- Contain characters from at least three of the following four categories:
    - English uppercase characters
    - English lowercase characters
    - Numbers
    - Non-alphabetic characters such as !, $, # etc.

Users are encouraged to change their password immediately if they are aware that security has been compromised.

In addition:-

- All staff and have a responsibility to ensure the security of their username and password. For example, whenever possible passwords should be memorised and not written down. If necessary, passwords may be written down if stored securely.
- Staff must not share their log in details with any other person or allow any other person to access school systems using their log in details.

- All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords e.g.
    - Do not write down system passwords.
    - When users are present, work stations may be logged in by the user to enable ICT support to troubleshoot existing problems.
    - When ICT support require access to a user's account when the user is not present, or on an ad hoc basis to resolve on-going errors, then ICT support will change the password centrally in order to provide adequate protection to both parties and comply with audit requirements.
    - Always use your own personal passwords to access computer based services, never share these with other users.
    - Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
    - Never save system-based usernames and passwords within an internet browser.
- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the school's personal data policy.
- The school maintains a log of all accesses by users and of their activities while using the system for a period of six months.
- Passwords must contain a minimum of eight characters and be difficult to guess.
- Users should create different passwords for different accounts and applications.
- Users should use numbers, letters and special characters in their passwords (! @ # $ % * ( ) - + = , < > : : " '): the more randomly they are placed, the more secure they are.

New and Emerging technologies

The school is committed to providing the best possible learning opportunities for all pupils and will regularly review and assess available technologies to ensure IT resources are relevant and of an appropriate specification to meet the needs of the curriculum and other related targets within the School Development Plan.

- New and emerging technologies will be assessed to determine:
    - Educational benefit. There must be documented evidence to inform the school's decision to proceed with any purchase, based on impact appraisal and additional benefits not already provided for within the school's IT resources.
    - Whether purchase would serve to address objectives within the School Development Plan.
    - Value for SEND use. Would purchase constitute a 'reasonable adjustment' in terms of access to the curriculum for any individual or group with special educational needs and disabilities?
    - All new technologies will be tested and reviewed for any security vulnerabilities that may exist. Appropriate control measures will be implemented within school to ensure that any risks are managed to an acceptable level.
- The school will periodically review which technologies are available within school for any security vulnerabilities that may have been discovered since deployment.
- All new technologies deployed within school will be documented within the e-safeguarding and Acceptable Use Policies prior to any use by any member of staff or pupil.
- The acceptable use of any new or emerging technologies in use within school will be reflected within the school e-safeguarding and Acceptable Use policies. All staff and pupils (when relevant) will be required to acknowledge receipt of changes incorporated into the Acceptable Use Policy as and when required.
- Prior to deploying any new technologies within school, staff and pupils will have appropriate awareness training regarding safe usage and any associated risks.
- The school will audit ICT equipment usage to establish if the e-safeguarding policy is adequate and that the implementation of the e-safeguarding policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Filtering internet access & monitoring

- The school currently procures filtering internet solutions through a third party company
- Content filtering will be overseen and managed by the ICT Technician. Settings will be differentiated for staff and pupils.
- All staff and pupils will be made aware that content will be monitored
- All staff and pupils will be encouraged to report inappropriate content to a key member of staff who will notify the ICT Technician.
- Through training and induction procedures, all staff will be made aware of reporting protocols in the event of inappropriate and/or illegal content
- The e-safety lead will take an active role in formally reporting incidents to the relevant authority
- The ICT Technician will be responsible for the day to day management of the school's filtering system; monitoring its effectiveness
- The school filtering system will block all sites on the Internet Watch Foundation. This is managed centrally by the current filtering solution provider.
- The school will enable access to specific websites on a time and location limited basis to facilitate learning, e.g access to Facebook to demonstrate e-safeguarding principles.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.
- Pupils will be taught to assess content as their internet usage skills develop.
- Pupils will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- Activity on school devices will be monitored using Senso. This will use keyword filters to pick up on any misuse of systems as well as potential safeguarding concerns

Internet and school network access authorisations

- All new members of staff will be expected to undertake e-safeguarding awareness training and to fully understand the implications of protecting themselves, the school and the school community before access to the school network and internet is granted.
- A summarised version of this policy will be provided to temporary staff employed on an ad hoc basis, students on work experience placements, volunteers and any visitor allocated a basic level of access to the school network and/or internet.
- All staff and work experience students will be expected to read, sign and comply with the school's Acceptable Use Policy.
- Permissions will be allocated to access areas of the school network at an appropriate level; determined by role.
- Members of staff with access to confidential pupil data and/or personnel data are charged with additional responsibilities in ensuring the Data Protection Act is complied with at all times.
- The school will maintain a current record of all staff and pupils who have been granted access to the school's network and internet provision.

Email

All members of staff will be issued with a school email account unless this facility is not required for the purposes of their particular post. School email accounts will be used for all school related communications. The use of personal email accounts is not permitted for this purpose and should not be accessed in school. The use of personal email accounts for communicating with any person within the school community or conducting any school related business is strictly prohibited. Similarly, school email accounts should not be used for personal use or communicating any matter which is not school business related.

- Email accounts should be used safely and appropriately in accordance with the school's Acceptable Use Policy.
- Effective and efficient communication methods will rely upon all staff accessing and checking their email account at least once per school day within normal working hours. Email will be used to circulate important and urgent information within specified time frames. For instance, signposting new policy and policy updates or requesting attendance at meetings.

- Staff should ensure that read receipt requests issued by the Headteacher (or on behalf of the Headteacher) are acknowledged
- Email accounts will be monitored and checked for appropriate use and to ensure staff access their accounts regularly.
- All email users will create a personal log-in for their account which will be changed at regular intervals in accordance with the school's password policy. Individuals will be responsible for the security of log-in details. These should never be shared with any other person.

Email usage

- Email accounts will only be used in accordance with the term and conditions of the school's Acceptable Use Policy.
- The content of sent and received emails may be subject to monitoring and should not be considered private.
- Individuals should maintain professional standards at all times when communicating by email both internally and externally. Emails should be courteous and
- Individual school email accounts should not be used for sending or receiving confidential information relating to pupils or staff. Approval should always be sought following requests for confidential or sensitive information.
- Addresses of intended recipients should always be checked for accuracy before sending emails.
- All staff and pupils will receive on-going relating to the school email system. Staff will be alerted to any specific threats or dangers encountered and to the dangers of opening suspicious emails and attachments
- The school's whistle blowing procedures will be followed in the event of any user receiving emails with inappropriate content from another user either within the same school or local authority.
- Inappropriate content received from an external source will be recorded and reported in accordance with the school's incident reporting procedures.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school'.
- All users will be responsible for managing their email account, ensuring that the folder system is used efficiently and emails no longer required are deleted.

Social Networking

The school uses Twitter and Facebook to share activity in school with the school community. This is managed by the Strategic Data Lead. A system is in place whereby staff are able to share content using the devices in the classroom. Any requests to post content is vetted and has to be approved by a member of SST. Photo consent is sought from parents where use of social media is defined as part of the agreement. The list of children who parents have given consent for, is shared with staff and updated regularly.

Personal social networking accounts

Members of staff who have an account with any social network (Facebook, Twitter etc.) should ensure that:-

- Their use complies fully with the terms of the school's AUP
- Accounts are not accessed on school premises using school equipment or accessed with personal devices during working hours
- Social networking sites are not used to express or communicate opinion relating to any aspect of the school.
- Privacy and security settings are checked regularly to ensure maximum protection (preferably allowing access to friends only and not 'friends of friends'). Staff should be aware that they cannot control content accessed by third parties
- They are aware that content should not impact negatively on their own professional standards.
- Pupils, either current or past (if under 18) and their families should not be accepted as friends. Staff should inform the Headteacher or e-safeguarding coordinator of pre-existing friendships with parents of pupils.

School issued laptops/tablets

The school routinely issues laptops to all teaching staff and, where appropriate, to members of support staff. Members of the SLT and Foundation stage teaching staff are also issued with tablet computers. All mobile devices are fully encrypted as a safeguarding measure to prevent unauthorised access. Members of staff issued with mobile devices are responsible for taking reasonable measures to prevent loss or damage:-

- Staff should ensure devices are connected to the school network on a regular basis (at least once per week) to ensure security updates and settings are applied and to synchronise folders.
- All laptops will be encrypted to safeguard against unauthorised access.
- Tablets can be remotely wiped if lost or stolen
- Staff are responsible for taking reasonable measures to protect school resources by:-
    - Not leaving portable devices in cars unless they have been locked in a boot.
    - Storing devices securely at home and ensuring they are not accessible by any other person when in use.
    - Not permitting any family member or friend to use the device

Use of Mobile phones in school

The school currently owns two mobile phones:-

1. One permanently issued to the caretaker
2. A mobile available for any member of staff to use on educational visits. This will be logged out to the relevant member of staff and used a means of emergency contact for the duration of the visit.

No other school owned mobile phones are deemed necessary. Individual members of staff will be responsible for any personal mobile telephone or device brought into school and cannot hold the school responsible for any loss, damage or theft. In all other aspects, members of staff will comply with the terms of the school's acceptable use policy:-

- Personal mobiles will not be used for any school related activity.
- Mobiles should be locked when not in use to prevent unauthorised use and set to silent mode. In exceptional circumstances permission from the Headteacher may be granted to receive or make emergency calls.
- Mobiles should not be used during hours of employment or at any other time when attending school related activities or business.
- Devices should only be used within specified areas referred to within the AUP
- Staff must not disclose their personal number to any child or parent. All telephone calls will be made using the school's land line, ensuring confidentiality is maintained at all times.
- Mobile phones must not be used for taking photographs, recording of audio or video on school premises or on any school related activity. The exception applies to members of staff who are also parents of children attending the school. As parents they are permitted to record

Data protection and information security

The school is registered with the Informational Commissioner's Office (ICO) as a data controller and carries out its duty of care in accordance with the Data Protection Act 1998. The school takes its responsibilities under the act seriously and is committed to ensuring compliance with the eight principles of data protection:-

1. *Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:-*
2. *(a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*
3. *Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.*
4. *Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.*
5. *Personal data shall be accurate and, where necessary, kept up to date.*
6. *Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.*
7. *Personal data shall be processed in accordance with the rights of data subjects under this Act.*

8. *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*
9. *Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.*

- All staff will undertake awareness training on induction and thereafter on a regular basis to refresh knowledge and take account of changes to legislation and/or school based procedures.
- Access to personal, confidential and sensitive information will be restricted on a 'need to know' basis determined by the Headteacher, SLT and SIRO.
- An on-going system of risk assessment will determine appropriate levels of security and electronic means required to control and minimise risk.
- The school has an established system of reporting breaches of security and/or wilful manipulation of data through its Whistle Blowing Policy and incident logging procedures.
- All staff will comply with the school's Acceptable Use Policy at all times in discharging their duty to protect data. This includes use both on and off site.
- All users should ensure they lock their computer when away from their desk or work area; the most commonly used method being Ctrl, Alt, Delete.
- Staff should be alert to unauthorised users viewing sensitive and/or personal information on their monitor or connected projector/screen. This is particularly relevant in areas where members of the public or visitors may be able to view monitor screens.
- The school has in place a secure and robust password policy which all members of staff and other authorised users will comply with.
- All staff, governors and visitors to the school will comply with the school's Acceptable Use Policy.
- All communications involving personal or sensitive information (email or post) should be appropriately secured.

Management and control of physical data

The school's commitment to data protection extends to all physical records containing personal data. Additional control measures to ensure the security of school data not held electronically have been put in place to ensure compliance with the Data Protection Act; namely:-

- All paper records will be stored in controlled access areas.
- All confidential and/or sensitive information relating to pupils and staff are stored in locked cabinets in either the Headteacher's office or the Deputy Headteachers' office.
- Paper records relating to budget management,

Management of assets

- The school holds an electronic inventory of all school owned hardware, including date of purchase, value at purchase, serial numbers and physical location within school.
- Hardware will not be moved from designated locations within the school without prior permission.
- Requests to take any device (which is not individually allocated) off site must be logged out and returned to the ICT technician.
- Where mobile devices have been allocated to individual members of staff (laptops and tablets), this will also be recorded within the inventory.
- An inventory is held of all school owned software and licences.
- All hardware will be security marked with chemical etching and/or 'Smart' water
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All disposals will be approved by the Headteacher, or, where the total value exceeds Headteacher's delegated authority; the governing body.

- Where the school has entered into a lease agreement for the provision of photo-copying and printing equipment, the provider will be asked to sign an undertaking that, on return of the equipment, all data will be permanently deleted from the hard-drive before disposal or transfer to any other person(s).
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

Storage of images

Any images, videos or sound clips of pupils must be stored on the school network. Images must not be stored on any personally owned device. All staff and other members of the school community will comply with the terms of the Acceptable Use Policy at all times; in particular, no individual will use personal equipment for any purpose relating to school activities.

Any third party (eg newspaper photographers, visitors from other schools) will require approval in advance. Third parties will also be required to provide evidence of their own data protection and data management protocols before permission is granted.

The school will ensure that stored images are not retained unnecessarily when pupils have left the school. Individual members of staff will be responsible for the following:-

- Each member of staff is responsible for ensuring images which need to be retained are transferred to the appropriate location on the school network on the school's server.
- Staff should take care to only transfer images which are required to ensure storage space is not used unnecessarily.
- All images held on SD cards should be deleted immediately following transfer to the server. If this is not feasible the same day, then the camera (with the SD card intact) should be held in a lockable storage cupboard until images can be safely transferred and deleted.
- Staff should be aware that images held on any portable device or school server are classed as personal data and should be protected accordingly (Data Protection Act).
- Any loss of data should be reported immediately to the school's SIRO.
- Staff should ensure that all users (including children) routinely delete images stored on digital devices once they have been transferred as described above.

Virtual Learning

Please see separate virtual learning policy

Review and ownership

- The e-safety lead will be responsible for updating and reviewing this document
- The school e-safeguarding policy has been agreed by the senior leadership team and approved by Governors

Lincoln Gardens Primary School's senior leadership team and governing body will ensure that any relevant or new legislation which may impact upon the provision for e-safeguarding within school will be reflected within this policy. This policy will be reviewed by governors on an annual basis in the Autumn term, or earlier, should it be necessary.

R Smith
September 2020