The Linden Centre

Online Safety Policy

Signed by:		
	Headteacher	Date:
	Chair of Management Committee	Date

Last Updated	04th January 2021
Review Due:	04th January 2022

Contents:

1. **Scope of the Policy**

This policy applies to all members of Linden Centre community (including staff, Pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the Linden Centre digital technology systems, both in and out of Linden Centre.

The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of Pupils when they are off the Linden Centre sites and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the Linden Centre schools, but is linked to the Linden Centre. The 2011 Education Act increased these powers concerning the searching for and of electronic devices and the deletion of data.

The Linden Centre will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

2. **Roles and Responsibilities**

The following section outlines the online safety roles and responsibilities of individuals and groups within the Linden Centre:

2.1. Management Committee

Management Committee is responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Management committee receiving regular information about online safety incidents and monitoring reports.

2.2. Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day

to day responsibility for online safety will be delegated to the Computing Subject Lead

- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

2.3. Network Manager/Technical staff

Those with technical responsibilities are responsible for ensuring:

- that the *school's/academy's* technical infrastructure is secure and is not open to misuse or malicious attack
- that the Linden Centre meets required online safety technical requirements online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the internet is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders for investigation/action/sanction

2.4. Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current Linden Centre online safety policy and practices

- they have read, understood and signed the staff acceptable use policy/agreement (AUP/AUA)
- they report any suspected misuse or problem to the Headteacher for investigation/action/sanction
- all digital communications with Pupils/parents/carers should be on a professional level
- online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Online Safety Policy and acceptable use policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned Pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

2.5. Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

2.6. Pupils:

- are responsible for using the Linden Centre digital technology systems in accordance with the student/pupil acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.

- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Linden Centre's online safety policy covers their actions out of school, if related to their membership of the school

2.7. Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The *Linden Centre* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature*. Parents and carers will be encouraged to support the *Linden Centre* in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform and on-line student/pupil records
- *their children's personal devices in the Linden Centre (where this is allowed)*

3. **Policy Statements**

3.1. Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of Pupils in online safety/digital literacy is therefore an essential part of the Linden Centre's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need to adopt safe and responsible use both within and outside Linden Centre.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that Pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where Pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs,

discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

3.2. Education – Parents/carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The Linden Centre will therefore seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, web site*

3.3. Education – The Wider Community

The Linden Centre will provide opportunities for local community groups/members of the community to gain from the school's/academy's online safety knowledge and experience. This may be offered through the following:

- The Linden Centre website will provide online safety information for the wider community
- Sharing their good practice with other local schools

3.4. Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the Linden Centre online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process. .
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.

3.5. Technical – infrastructure/equipment, filtering and monitoring

The Linden Centre will be responsible for ensuring that the Linden Centre infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities: .

- Linden Centre technical systems will be managed in ways that ensure that the Linden Centre meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of Linden Centre technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to Linden Centre technical systems and devices.
- All users will be provided with a username and secure password by IT Support who will keep an up to date record of users and their usernames.
- Users are responsible for the security of their username and password.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten

the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.

- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

3.6. Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behavior policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

3.7. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and Pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and Pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate Pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of Pupils are published on the school website/social media/local press
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow Linden Centre policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Linden Centre equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that Pupils are appropriately dressed and are not participating in activities that might bring the individuals or the Linden Centre into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include Pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

4. **Communications**

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

When using communication technologies, the Linden Centre considers the following as good practice:

- The official Linden Centre email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and Pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the Linden Centre website and only official email addresses should be used to identify members of staff.

4.1. Social Media - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *Linden Centre* or local authority/MAT liable to

the injured party. Reasonable steps to prevent predictable harm must be in place.

The Linden Centre provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Linden Centre staff should ensure that:

- No reference should be made in social media to Pupils, parents/carers or Linden Centre staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to The Linden Centre
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

4.2. Personal Use:

- Personal communications are those made via a personal social media account,. In all cases, where a personal account is used which associates itself with the Linden Centre or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the Linden Centre with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

4.3. Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process
- The Linden Centre's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

5. Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from Linden Centre and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a Linden Centre context, either because of the age of the users or the nature of those activities.

The Linden Centre believes that the activities referred to in the following section would be inappropriate in a Linden Centre context and that users, as defined below, should not engage in these activities in/or outside the Linden Centre when using Linden Centre equipment or systems.

6. Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities

7. Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity report immediately to the police.

8. **Other Incidents**

It is hoped that all members of the Linden Centre community will be responsible users of digital technologies, who understand and follow School policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour

- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- offences under the Computer Misuse Act (see User Actions chart above)
- other criminal conduct, activity or materials

- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the *Linden Centre* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

9. **Linden Centre actions & sanctions**

It is more likely that the Linden Centre will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.