Internet Safety Policy

Date Policy Reviewed:	**January 2018**
Date Approved by Governing Body:	**February 2018**
Date of Next Review:	**September 2019**

Introduction

At Longfield Academy we are working with the Directors, Staff, Pupils and Parents/ Carers to create a school community which:

- Values the use of new technologies in enhancing learning
- Encourages responsible use of ICT
- Follows agreed policies to minimise potential E-Safety risks

Rationale

We aim as a school to hit the DFE recommendations that: ***"An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate".*** The so-called 'new' technologies are central to both our lives and those of children and young people in today's society, both in school and outside.

Electronic communication helps teachers and pupils learn from each other and the wider world, and the technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is a part of the wider duty of care by which all who work in schools are bound. It is important for the school to protect pupils and staff alike from the following issues within school:

"The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:
• Content: being exposed to illegal, inappropriate or harmful material;
• Contact: being subjected to harmful online interaction with other users; and
• Conduct: personal online behaviour that increases the likelihood of, or causes, harm". (Keeping Children Safe in Education 2016, page 62) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/550511/Keeping_children_safe_in_education.pdf

We recognise that the continuing development and implementation of this strategy must involve all the stakeholders in a child's education from the Head Teacher and Directors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves if it is to be successful.

The use of new technologies in school and at home has been shown to raise educational standards and promote pupil achievement. We recognise that the internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. But these opportunities are not without risk.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The risk of being subject to radicalisation
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the off-line world and it is essential that this E-Safety Policy is seen and understood to operate in conjunction with other school policies which can all be viewed via our website.

As with all other risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

We recognise that we must provide the necessary safeguards to help ensure we have done everything that could reasonably be expected in order to manage and reduce these risks. Our Internet Safety Policy explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their Parents / Carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Scope of the Policy

This Policy applies to all members of the school community (including staff, pupils, volunteers, Parents/Carers, visitors, community users) who have access to and are users of school ICT systems.

The school will deal with E-Safety incidents and associated behaviour and anti-bullying policies and will, where known, inform Parents/Carers of incidents of inappropriate E-Safety behaviour. Help and advice can be provided to Parents by the school via the

school website E-Safety tab where links to CEOPS www.ceop.police.uk, twitter.com/ceopuk and www.ceop.police.uk/safety-centre, Childline www.childline.org.uk, www.thinkyouknow.co.uk, the Internet Watch Foundation www.iwf.org.uk and How to get safe online www.getsafeonline.org are all available. This will help pupils and parents alike to stay safe online and inform them of how to report incidents when they have happened outside of school time on personal devices, through personal accounts. The DFE also states through the Keeping Children Safe (2016) document that the following websites can also provide support and advice:

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

www.pshe-association.org.uk

www.educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Roles and Responsibilities

The following section outlines the roles and responsibilities for E-Safety of individuals and groups within the school.

Local Governing Body:

A specified member of the Local Governing Body should take on the role of E-Safety link director. The role of the Internet Safety Governor will include:

- Regular meetings with the Internet Co-ordinator / Officer, Chris Carr
- Reporting to relevant committees / meetings

Head of School and Senior Leaders:

- The Head of School is responsible for ensuring the safety (including Internet-Safety) of members of the school community, though the day to day responsibility for Internet-Safety will be delegated to the Safeguarding Team
- The Senior Leadership Team are responsible that for ensuring relevant staff receive suitable CPD to enable them to carry out their Internet-Safety roles and to train other colleagues, as relevant
- The Head of School will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Internet-Safety

monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Head of School and other members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Internet-Safety allegation being made against a member of staff

Internet-Safety Coordinator/Officer:

- Longfield has a two named Internet Safety Ambassadors – there are Amanda Payne and Peter Haylock

These people:

- Lead on Internet-Safety matters in school
- Take day to day responsibility for Internet-Safety issues and have a leading role in establishing and reviewing the school Internet-Safety Policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Internet-Safety incident taking place
- Provide training and advice for staff in cooperation with Safeguarding officers in school
- Liaise with the Local Authority where appropriate and necessary
- Liaise with school ICT technical staff
- Receive reports of Internet-Safety incidents and create and keep a log of incidents to inform future Internet-Safety development
- Meet regularly with Internet Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- Attend relevant meeting / committee of Local Governing Body
- Peter Haylock will provide an annual report that will illustrate any Internet-Safety issues and trends that may be occurring within school

Incidents that infringe the Internet-Safety Policy will be dealt with according to their severity. The investigation / action / sanctions in case of pupil infringement of the policy will be dealt with via the school systems, but any major incident or incidents involving any employee or Parent/Carer or community user must be reported immediately to the Safeguarding Team.

In the case of pupils the full range of school sanctions are open to the Head of School for deliberate infringement of the Policy, up to and including fixed term or permanent exclusion. If an incident has occurred outside of school then a full range of support/ advice is provided to parents about actions that should be taken and where to report incidents or seek advice (please refer to the scope of the Policy section).

In the case of staff the full range of disciplinary responses are open to the Head of School for deliberate infringement of the Policy, up to and including recommending dismissal.

In the case of infringement by Parents/Carers or community users the Head of School will refer the matter to the appropriate external agency via the Children's Access Point, Multi-Agency Safeguarding Hub or the Police.

Network Manager and Technical staff:

The Network Manager is responsible for ensuring:

- That the school's IT infrastructure is secure and is not open to misuse or malicious attack
- That the school meets the Internet-Safety technical requirements
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- The school's filtering system, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- He keeps up to date with Internet-Safety technical information in order to effectively carry out his Internet-Safety role and to inform and update others as relevant
- That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Internet-Safety Coordinator for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies
- That all staff are informed of the importance of password protecting their won devices used for school data

Teaching and Support Staff

The DFE Keeping Children Safe (2016) document states ***"Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 64) and the requirement to ensure children are taught about safeguarding, including online (paragraph 68), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach".*** Staff training is provided on Inset days related to Safeguarding as well as Internet-Safety.

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of Internet-Safety matters and of the current school Internet-Safety policy and practices
- They have read, understood the school Policy on use of ICT (Acceptable User Policy, AUP)
- They report any suspected misuse or problem to the Internet-Safety Coordinator for investigation / action / sanction
- Digital communications with pupils should be on a professional level and only carried out using official school systems

- Internet-Safety issues are embedded in all aspects of the curriculum and other school activities
- Staff understand and follow the school Internet-Safety and acceptable use policy
- Staff have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They are aware of Internet-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school 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

Designated Person for Child Protection and Safeguarding

Designated Child Protection trained staff must be trained in Internet-Safety issues and be aware of the potential for serious child protection 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
- Cyber-bullying

When dealing with a Sexting incident Pastoral staff should follow the guidance from The UK Council for Child Internet Safety 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'. This can be found on the following website: https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Pupils:

- Are responsible for using the school ICT systems in accordance with the AUP, which they electronically accept on entry to the school internet / network
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber- bullying
- Should understand the importance of adopting good Internet-Safety practice when using digital technologies out of school

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.

Parents and carers will be responsible for:

- Accessing the school website / on-line pupil records in accordance with the relevant school AUP

Community Users

Community Users who access school ICT systems / website as part of the Extended School provision will be expected to sign a **Community User Acceptable User Policy. This will also apply to temporary members of teaching staff. The Network Manager will hold a register of users and their signed agreement to abide by school policy. In addition all users will have to agree to the policy electronically on entrance to the school ICT network.**

Education of pupils

We believe that 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 Internet-Safety is therefore an essential part of our school's Internet-Safety provision. Children and young people need the help and support of the school to recognise and avoid Internet-Safety risks and build their resilience.

Internet-Safety education will be provided in the following ways:

- A planned Internet-Safety programme is provided.
- Key Internet-Safety messages are reinforced as part of a planned programme of assemblies and PSHE activities
- Pupils are explicitly taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Pupils are helped to understand the need for the AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both in and outside school
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff are expected to act as good role models in their use of ICT, the internet and mobile devices

Education – Parents/Carers

Many Parents and Carers have only a limited understanding of Internet-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 on-line experiences.

Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. Parents also sometimes find it difficult to know which Apps or websites their children are accessing and using. “There is a generational digital divide”. (Byron Report).

The school provides information and awareness to Parents and Carers through:

- Parental Internet-Safety awareness evenings
- Web site – which provides parents with help and support with how to educate pupils, how to report incidents and how to educate themselves
- Parents evenings
- Signposting to further areas of support

Education and Training – Staff

We regard it as essential that all staff receive Internet-Safety training and understand their responsibilities, as outlined in this Policy. Training will be offered as follows:

- It is expected that some staff will identify Internet-Safety as a training need within the Appraisal process
- All new staff will receive Internet-Safety training as part of their induction programme via their safeguarding briefing and awareness session (NQT / New staff induction programme), ensuring that they fully understand the school’s Internet-Safety policy and AUP
- The Internet-Safety Coordinator/Officer should receive regular updates through attendance at LA and other information / training sessions and by reviewing any guidance documents
- The Internet- Safety Coordinator/Officer (or other nominated person) will provide advice / guidance / training as required to individuals as required

Training – Local Governing Body

Governors should take part in E-Safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in ICT / Internet-Safety / Health and Safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Directors Association or other relevant organisation
- Participation in school training / information sessions for staff or parents
- Technical – infrastructure / equipment, filtering and monitoring

Responsibility of the School

- The school will be responsible for ensuring that the school infrastructure/ network is as safe and secure as is reasonably possible and that policies and procedures approved within this Policy are implemented
- School ICT systems will be managed in ways that ensure that the school meets the Internet-Safety technical requirements outlined in any relevant Local Authority / government Internet-Safety Policy and guidance.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager
- All users will be provided with a username and password by the Network Manager or nominated member of the Network Team. The Network Manager will keep an up to date record of users and their usernames
- The “master / administrator” passwords for the school ICT system, used by the Network Manager must also be available to the Head of School or other nominated Senior Leader and kept in a secure place (e.g. school safe)
- Users are responsible for the security of their username and password, and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The school has provided enhanced user-level filtering
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the a member of the Safeguarding system
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and Internet- Safety Co-ordinator. If the request is agreed, this action will be recorded
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the AUP
- Remote management tools are used by staff to control workstations and view users’ activities
- The school discipline system shall be used for users to report any actual / potential Internet-Safety incident to the Internet-Safety Co-ordinator / Network Manager when this occurs in school time
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on

laptops and other portable devices that may be used out of school. This is administered and held by the Network Manager
- The school infrastructure and individual workstations are protected by up to date virus software
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured and with the permission of the Internet-Safety Co-ordinator
- To provide parents, staff and pupils alike on where to gain advice and help on Internet-Safety issues

Curriculum

Internet-Safety is a focus in all areas of the curriculum and staff are expected to reinforce E-Safety messages in the use of ICT across the curriculum.

- 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
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff are expected to be vigilant in monitoring the content of the websites the young people visit. Staff will be expected to monitor pupil's activity using the Impero system installed in all ICT rooms
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager 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
- Pupils are 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 are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet.

Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school informs and educates users about these risks and implements policies to reduce the likelihood of the potential for harm:

- When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular pupils are taught to recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Staff are allowed to take digital / video images to support educational aims, but must follow the school policy concerning the sharing, distribution and publication of those images
- Those images should only be taken on school equipment; 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 school 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
- Written permission from Parents/Carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and Parents/ Carers

Data Protection

Personal data will be recorded, processed, transferred and made available according to the ***Data Protection Act 1998*** which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

Dealing with breaches of the Policy

Any use that contravenes this policy will be dealt with by the standard disciplinary routes and may involve withdrawal of ICT usage privileges and potential disciplinary action. These sanctions will be applied at the discretion of the Head of School.

Internet-Safety incidents involving students will be reported via the normal referral routes. Any incident will then be recorded on the SIMS system in the behaviour management area.