LANTERN OF KNOWLEDGE

EDUCATIONAL INSTITUTE

# LoK E-Safety Policy

July 09

# 2023

Revised by S. Ahmed

| | | Next Review Date | Sep 2025 |
|---|---|---|---|
| | | | |
| Responsible Person | Position | Date | Sign |
| Shakil Ahmed | Headteacher | 09/07/2023 | |
| Ml Irfan Sidyot | Governor | 09/07/2023 | |
| | | | |

# E-Safety Policy

## The Acceptable use of the Internet and related technologies

Table of Contents

Our E-Safety Policy has been written by building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance.

# 1. E- Safety Overview

We have a duty to ensure that all pupils are able to make a valuable contribution to society & this is impossible to achieve if we do not ensure that pupils develop and apply their ICT capability effectively in their everyday lives.

The school is aware of its responsibilities in ensuring that ICT usage by all network users is responsible, safe and secure. There are relevant and comprehensive policies in place which are understood and adhered to by many network users.

Most pupils have a good range of skills that enables them to access and make effective use of digital resources to support their learning. They understand the issues relating to safe and responsible use of ICT and adopt appropriate practices.

Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstance. However, there are some pupils, for example looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online. Pupils with such vulnerabilities will have additional measures identified and recorded in their pupil passports (and where relevant in the curriculum maps).

*Harnessing Technology: Transforming learning and children's services* [1] sets out the government plans for taking a strategic approach to the future development of ICT.

*"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.*

*To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom."* DfES, eStrategy 2005

The Green Paper *Every Child Matters*[2] and the provisions of the *Children Act 2004*[3], *Working Together to Safeguard Children*[4] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

[1] http://www.dfes.gov.uk/publications/e-strategy/

[2] See The Children Act 2004 [http://www.opsi.gov.uk/acts/acts2004/20040031.htm]

[3] See Every Child Matters website [http://www.everychildmatters.gov.uk]

[4] Full title: Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children. See Every Child Matters website [http://www.everychildmatters.gov.uk/_files/AE53C8F9D7AEB1B23E403514A6C1B17D.pdf]

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the School to ensure that every child in its care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the School's physical buildings.

This policy document is drawn up to protect all parties – the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

## 1.1 The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (e.g. http://www.facebook.com )
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com )
- Gaming Sites (Popular www.neopets.com )
- Music download sites (Popular http://www.apple.com/itunes/ )
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.
- On-line gaming e.g via Wii, PS3, Xbox and similar technologies
- Twitter
- Instagram
- Tik Tok
- Snapchat
- WhatsApp
- Kick

## 1.2 Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for pupils, staff and parents.

The school will ensure online safety is a running and interrelated theme whilst devising and implementing policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the DSL and any parental engagement.

*Ref: Becta - E-safety Developing whole-school policies to support effective practice* [5]

## 1.3 Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the policy is implemented and compliance with the policy monitored. The responsibility for e-Safety has been designated to a member of the senior management team.

Our school e-Safety Co-ordinator is Sohale Saber (Computer Science Teacher)

Our e-Safety Coordinator ensures he keeps up to date with e-Safety issues through the Local Authority e-Safety web site and other organisations such as The Child Exploitation and Online Protection (CEOP)[6]. The school's e-Safety coordinator ensures the Head, other senior leaders and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance [7] on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with school policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil/staff information/photographs and use of website;
- e-Bullying / Cyberbullying procedures;
- their role in providing e-Safety education for pupils;

[5] http://schools.becta.org.uk/index.php?section=is
[6] http://www.ceop.gov.uk/
[7] Safety and ICT - available from Becta, the Government agency at: http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_str_02&rid=10247

Staff are reminded / updated about e-Safety matters at least once a year.

The school includes e-safety in the curriculum and ensures that every pupil has been educated about safe and responsible use. Pupils need to know how to control and minimise online risks and how to report a problem.

The school makes every effort to engage with and inform parents over e-safety matters and requires all parents/carers to sign and return an e-safety/AUP form.

## 1.4 Communications

### How will the policy be introduced to pupils?

Many pupils are very familiar with the culture of new technologies but their perceptions of the risks may not be mature. Therefore an e-safety training programme has been introduced to raise the awareness and importance of safe and responsible internet use.

On joining the school every pupil has the Acceptable Use Policy explained to them. All pupils sign two copies of the AUP, one for their own use and one which is retained by the school.

The e-safety rules are reinforced through explanation and discussion in ICT lessons and in PHSE/Citizenship lessons throughout the year groups. In particular instruction in responsible and safe use precedes Internet access.

Work in ICT is supplemented through the PSHE/Citizenship programme for example when considering Bullying/Anti-Bullying.

### How will the policy be discussed with staff?

It is important that all staff, whatever their role, feel confident to use new technologies in their work. ICT use is widespread and all staff are entitled to appropriate awareness raising and training. Induction of new staff includes a discussion of the school's e-Safety Policy and explanation of the staff Acceptable Use Policy. All members of staff sign two copies of the AUP, one for their own use and one which is retained by the school.

In particular staff are made aware that:

- Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential, particularly as monitoring becomes more sophisticated.
- Colleagues who manage filtering systems or monitor ICT are supervised by senior management and have clear procedures for reporting issues.
- Training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required, including opportunities to discuss any issues and develop appropriate teaching strategies
- There are clear rules for information systems misuse.
- If they are concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

### How will parents' support be enlisted?

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school will try to help parents plan appropriate supervised use of the Internet at home by following the following principles:

- Internet issues will be handled sensitively, and parents will be advised accordingly.

- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

1.5 How will complaints regarding E-Safety be handled?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the School nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by tutor / e-Safety Coordinator / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period,
- referral to Police / LADO/Social Services/Channel/PMAP.

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

## 2. Managing the Internet Safely

2.1 Why is Internet access important?

The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment; indeed ICT is now seen as a functional, essential life-skill along with English and mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information.

The Internet provides many benefits to pupils and the professional work of staff through, for example:

- access to world-wide educational resources, including museums and art galleries;
- access to experts in many fields for pupils and staff;
- educational and cultural exchanges between pupils world-wide;
- collaboration between pupils, professionals and across sectors;
- access to learning wherever and whenever convenient.

The Internet enhances the school's management information and business administration systems through, for example:

- communication systems;
- improved access to technical support, including remote management of networks and automatic system updates;
- online and real-time 'remote' training support;
- secure data exchange between local and government bodies.

## 2.2 The risks

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere.

In line with school policies that protect pupils from other dangers, the school attempts to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This is within a 'No Blame' culture which encourages pupils to report abuse.

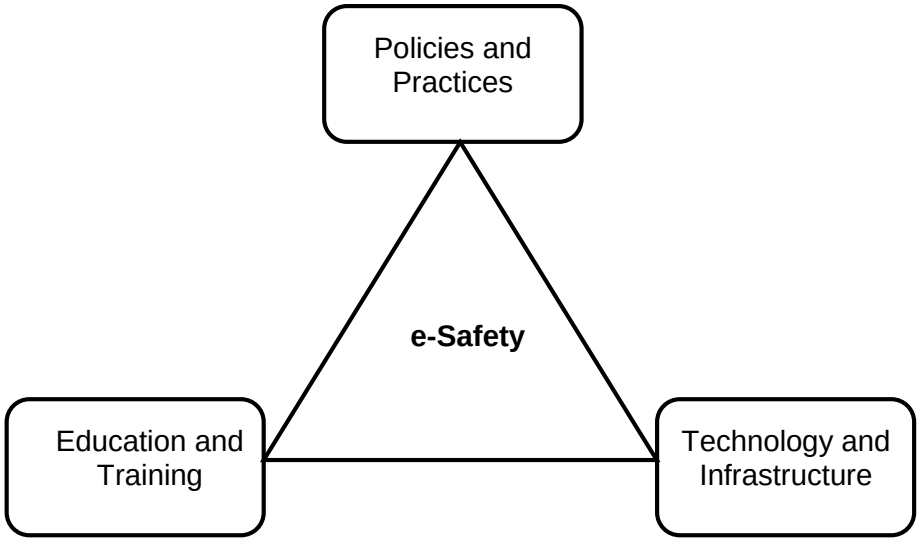
The School also makes it clear to all ICT users that the use of school equipment to view or transmit inappropriate material is "unauthorized" and infringements will be dealt with. We also try to ensure that all reasonable and appropriate steps have been taken to protect pupils, including technical and policy actions and an education programme for pupils, staff, and parents.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, pupils or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

There are three core elements to address for whole school e-safety:

- Technology
- Policy and Practices
- Education and training




2.3 Technology and Infrastructure

Lantern of Knowledge School:

- Ensures network health through appropriate anti-virus software etc and network set-up so staff and pupils cannot download executable files such as .exe / .com / .vbs etc.;
- Utilises caching as part of the network set-up;
- Ensures the Systems Administrator / network manager is up-to-date with services and policies;
- Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allows pupils access to Internet logs;
- Uses individual log-ins for all pupils and all other users;
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Never sends personal data over the Internet unless it is secure
- Uses 'safer' search engines with pupils such as http://yahooligans.yahoo.com/ | http://www.askforkids.com/ and activates 'safe' search where appropriate;
- Ensures pupils only publish within appropriately secure learning environments such as their own closed secure portal or Learning Platform.

2.4 Policy and practice

Lantern of Knowledge School:

- Supervises pupils' internet use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access;
- We use filtering systems which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- We have additional user-level filtering.
- Staff preview sites that they plan to use for learning before use or only use sites accessed from managed 'safe' environments;

- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google or yahoo image search;
- Informs users that Internet use is monitored;
- Informs staff and pupils that that they must report any failure of the filtering systems directly to the system administrator.
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes;
- Requires all pupils and their parent/carers to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme;
- Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named child protection officer has appropriate training;
- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their son's entry to the school;
- Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

2.5 Education and training

Lantern of Knowledge School:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report abuse;
- Has a clear, progressive e-safety education programme throughout both Key Stages, built on LA / London / national guidance in which pupils are taught a range of skills and behaviours appropriate to their age and experience.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;
- Ensures staff understand data protection and general ICT security issues linked to their role and responsibilities
- Makes training available annually to staff on the e-safety education program;

- Provides advice and guidance for parents, including:
    - Information leaflets; in school newsletters; on the school web site;
    - demonstrations, practical sessions held at school;
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.

## 3. Managing E-mail

At Lantern of Knowledge School:

- We do not publish personal e-mail addresses of pupils or staff on the school website.
- If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law we contact the police.
- Accounts are managed effectively, with up to date account details of users.
- Messages relating to or in support of illegal activities will be reported to the relevant authority and police.
- We use the anti-virus products.

Pupils:

- We do not use email that identifies the name and school of the pupil.
- Pupils can only use the school domain e-mail accounts on the school system.
- Pupils are introduced to, and use e-mail as part of the Computing scheme of work.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and more generally (for example personal accounts set-up at home)
- Pupils sign the school AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff use Microsoft e-mail systems for professional purposes – this is currently 'Outlook'
- Staff are only allowed to use the Staff mail e-mail accounts for school business
- Staff know that e-mail sent to an external organization must be written carefully, (and may require authorization), in the same way as a letter written on school headed paper. That it should follow the school 'house-style';
- All staff sign our school AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

## 4. Use of digital and video images

At Lantern of Knowledge School:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information is restricted to the webmaster
- The school web site complies with the school's guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their son joins the school;
- We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- Pupils are only able to publish to their own 'safe' web-portal in school;
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computer Science scheme of work;
- Pupils are taught about how images can be abused in their e-Safety education programme;

## 5. Social networking and personal publishing

At Lantern of Knowledge School:

- The school will block access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location.
- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas.
- Staff's official blogs or wikis should be password protected and run from the school website. Staff will be advised not to run social network spaces for pupil use on a personal basis.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others.
- Pupils will be advised not to publish specific and detailed private thoughts.
- Pupils and staff are made aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

## 6. Managing Equipment

6.1 Using the school network, equipment and data safely: general guidance

The computer system / network is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

*The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.*

To ensure the network is used safely Lantern of Knowledge School:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password;
- Provides pupils with an individual network log-in username. They are also expected to use a personal password;
- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find it;
- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Makes clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed.
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed;
- Has separate curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems.
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems e.g. technical support
- Follows advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school ICT systems regularly with regard to security.

## 7. Handling Infringements

Whenever a pupil or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

## 8. Pupils

Generally speaking pupil infringements of the e-Safety policy should be dealt with by following the school's behaviour policy which categorises negative behaviours into 5 levels (Level 5 being the most serious).

The following examples are provided as exemplification only:

8.1 Level 1 infringement

- Use of non-educational sites during lessons
- Unauthorised use of email
- Use of unauthorised instant messaging / social networking sites
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends

*[Possible Sanctions: To be dealt with by adult currently supervising the pupil following school behaviour policy, sanctions appropriate for Level 1 offences to be used. For use of mobile phone the school policy on confiscation should be followed]*

8.2 Level 2 infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups
- Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

*[Possible Sanctions: To be dealt with by adult currently supervising the pupil following school behaviour policy, this may merit referral to the Head Teacher. Sanctions as outlined for level 2 offences may also include removal of Internet access rights for a period and/or contact with parent]*

8.3 Level 3 infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or message that is regarded as harassment or of a bullying nature including to another member of the school community when outside school (one –off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

[Possible Sanctions: To be dealt with by adult currently supervising the pupil following school behaviour policy, this will usually merit referral to Head Teacher. Sanctions as outlined for level

3 offences may also include removal of Internet access rights for a period and/or contact with parent]

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform Systems Administrator as appropriate

8.4 Level 4/5 infringements

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned (including to another member of the school community when outside school)
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act GDPR 2018
- Bringing the school name into disrepute

*[Potential Sanctions – Must be referred to Head Teacher. Sanctions to be considered as for level 4/5 offences in Behaviour Policy. This will include contact with parents / possible internal isolation or external exclusion / removal of equipment / refer to Community Police Officer / Social Services]*

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider

## 9. Staff

Generally speaking staff infringements of the e-Safety policy should be dealt with in one of two ways:

Less serious infringements can often be dealt with informally, while more serious issues may need to be dealt with by following the school's disciplinary policy. Issues related to child protection would be dealt with using the school's child protection procedures. The following examples are provided as exemplification only:

9.1 Category A infringements

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the world wide web that compromises the staff member's professional standing in the school and community.
- Misuse of first level data security, e.g. wrongful use of passwords.

- Breaching copyright or license e.g. installing unlicensed software on network.

*[Potential Sanctions - referral to line manager /e-safety co-ordinator/ Headteacher. Verbal warning given, written note of expectation on personnel file.]*

9.2 Category B infringements

- Serious misuse of, or deliberate damage to, any school computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, sexist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

*[Sanction – Referred to Headteacher / Governors and follow school disciplinary procedures; report to LADO, potentially report to Police or Social Services]*

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.

If it is suspected that a member of staff may have committed an exceptionally serious breach of e-safety policy then the school's disciplinary policy allows for the member of staff to be suspended while an investigation takes place. In such cases suspension should be considered a neutral act which does not imply that the complaint has already been proven. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

The school is likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority.

9.3 Child Pornography found

In the case of Child Pornography being found, the member of staff should be immediately suspended and the Police should be called: see the free phone number 0808 100 00 40 at: http://www.met.police.uk/childpornography/index.htm

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

http://www.iwf.org.uk

9.4 How will staff and pupils be informed of these procedures?

- They will be fully explained and included within the school's e-safety / Acceptable Use Policy. All staff will be required to sign the school's AUP form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate AUP form;
- The school's e-safety policy will be made available and explained to parents, and parents will sign an AUP form when their child starts at the school.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if?' guide on e-safety issues, (see Guidance section below).

## 10. Guidance

10.1 Safeguarding and Protecting Children

What are the e-safety issues?

Although the use of ICT and the internet provide ever increasing opportunities for children to expand their knowledge and skills, it is also the case that the use of such technology may sometimes expose children to the risk of harm.

Apart from the risk of children accessing internet sites which contain unsuitable material, risks to the well-being of children may also exist in a variety of other ways.

It is known that adults who wish to abuse may pose as children to engage and then meet up with the children or young people they have been in communication with.
This process is known as 'Grooming' whereby an adult prepares a child or young person to be abused. The process may take place over a period of months using chat rooms, social networking sites and mobile phones.

An adult may pretend to be a peer and gradually convince the child or young person that they are their boyfriend or girlfriend, establishing a relationship of apparent trust with the intended victim and making it difficult for the child to then speak out.

Increasingly bullying is conducted on the internet or by the use of text messages and is therefore harder for schools to notice and deal with.

Section 175 of the 2002 Education Act and Section 11 of the 2004 Children Act places upon all those who work with children a duty to safeguard and promote their welfare by creating a safe learning environment and where there are child welfare concerns, taking swift action to address them.

It is vital that all adults working in schools are aware of the signs which might indicate that a child is being groomed, bullied or being subjected to inappropriate material and know how to take steps to begin to address this and safeguard and support the child.

In order to create a safe learning environment Lantern of Knowledge School has a comprehensive Safeguarding and Child Protection policy in place. This is reviewed annually and should be followed by all staff, teaching and non-teaching whether in a paid or voluntary capacity.

If you are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child, you should

- Ensure you follow the school's child protection procedures in any dealings you have with the child.
- Report the matter to the designated child protection officer immediately.
- The CPO will decide on the subsequent course of action in line with the school/LA and All London child protection procedures.

## 10.2 Cyberbullying

Cyber bullying is bullying through the use of communication technology such as mobile phone text messages, e-mails or websites. This can take many forms for example:

- Sending threatening or abusive text messages or e-mails, personally or anonymously
- Making insulting comments about someone on a website, social networking site or online diary (blog)
- Making or sharing derogatory or embarrassing videos of someone via mobile phone or e-mail)

It should be noted that the use of ICT to bully could be against the law.
Abusive language or images, used to bully, harass or threaten another, whether spoken or written (through electronic means) may be libellous, may contravene the *Harassment Act 1997 or the Telecommunications Act 1984* for example.

In order to tackle instances of bullying Lantern of Knowledge School has a comprehensive Anti-Bullying policy in place. This is reviewed annually and should be followed by all staff, teaching and non-teaching whether in a paid or voluntary capacity.

The Anti-Bullying Policy covers issues surrounding cyber bullying and makes it clear that the use of the web, text messages, e-mail, video or audio to bully another pupil or member of staff whether on or off school premises will not be tolerated.

Additionally staff may wish to consider the following guidance:

If a bullying incident directed at a child occurs using email or mobile phone technology either inside or outside of school time.

- Advise the child not to respond to the message
- Refer to relevant policies including e-safety/acceptable use, anti-bullying and behaviour and apply appropriate sanctions
- Secure and preserve any evidence

- Inform the sender's e-mail service provider
- Notify parents of the children involved
- Consider informing the police depending on the severity or repetitious nature of offence

If malicious or threatening comments are posted on an Internet site about pupils or staff

- Inform and request the comments be removed if the site is administered externally
- Secure and preserve any evidence
- Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html
- Endeavour to trace the origin and inform police as appropriate
- The school may wish to consider delivering a parent workshop for the school community

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

10.3 What do we do if?

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/e- safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is blocked.

An inappropriate website is accessed intentionally by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you; do not view the misuse alone.
2. Report the misuse immediately to the head teacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head teacher should then:
   - Remove the PC to a secure place.
   - Instigate an audit of all ICT equipment by the schools ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action if necessary.
   - Inform governors of the incident if necessary.
4. In an extreme case where the material is of an illegal nature:
   - Contact the local police or High Tech Crime Unit and follow their advice.
   - If requested to, remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety, anti-bullying and PSHE and apply appropriate sanctions.

1. Secure and preserve any evidence.
2. Inform the sender's e-mail service provider.
3. Notify parents of the children involved.
4. Consider delivering a parent workshop for the school community.
5. Inform the police if necessary.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.

All of the above incidences must be reported immediately to the head teacher and e-safety officer.

# 11. Acceptable Use Policies (AUP)

11.1 Acceptable Use Policy: Parents

As the parent or legal guardian of

…….. (Insert pupil's name)

I grant permission for my son to have access to use the Internet, e-mail and other ICT facilities at school.

I know that my son has signed an acceptable use policy form agreeing to its conditions and that this acceptable use policy contains 12 'rules for responsible ICT use'.

I have read the AUP for pupils and have discussed the rules for acceptable use with my child.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

I understand that the school can check my child's computer files, and the Internet sites they visit and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I also understand that should my child fail to follow the acceptable use policy the school will take appropriate action in line with the school Behaviour Policy.

Complaints about cyber bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to Child Protection are dealt with in accordance with school/local authority child protection procedures.

11.2 Acceptable Use Policy: Pupils

As a responsible member of Lantern of Knowledge School, I

…… (Insert pupil's own name). Have read and understand the rules below and agree to keep them.

TWELVE RULES FOR RESPONSIBLE ICT USE

1. I will only use the school's computers for schoolwork, homework and as directed.
2. I will not bring files into school (on removable media or online) without permission or upload inappropriate material to my workspace.
3. I will only edit or delete my own files
4. I will not view other people's files without their permission.
5. I will keep my logins, IDs and passwords secret.
6. I will use the Internet responsibly seeking permission from a member of staff before I do so. I will not visit or attempt to visit web sites I know to be banned by the school.
7. I will only e-mail people I know, or those approved by my teachers.
8. The messages I send, or information I upload, will always be polite and sensible.
9. I will not open attachments, or download a file, unless I have permission or I know and trust the person that has sent them.
10. I will not give my home address, phone number, send photographs or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
11. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me (i.e my parents or guardians).
12. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will save it and talk to a teacher / trusted adult.

IN ADDITION

13. I am aware that some websites and social networks have age restrictions and I should respect this.
14. I am aware that my online activity at all times should not upset or hurt other people including other pupils and members of staff
15. I am aware that I should not put myself at risk through my on-line activity at any time.
16. I also understand that should I fail to follow the acceptable use policy the school will take appropriate action in line with the school Behaviour Policy.
17. Complaints about cyber bullying are dealt with in accordance with our Anti-Bullying Policy.
18. Complaints related to Child Protection are dealt with in accordance with school/local authority child protection procedures.

11.3 Acceptable Use Policy: Staff

…… (Insert staff member's name)

I have read and understand the rules below and agree to keep them.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my username and password(s) to anyone else.
- I will not allow unauthorised individuals to access email / Internet / intranet / network.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business. (currently: Microsoft Outlook)
- I will only use the approved school email or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the network manager who will log the incident and take appropriate action.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer or laptop to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using appropriate anti-virus software.
- I understand that USB flash drives should be scanned before being used on the school network.
- I will not take and transfer images of pupils or staff on personal digital cameras or camera phones. I will not store images at home of staff or pupils.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected and that I follow school data security protocols when using it.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I will embed the school's e-safety curriculum into my working practice.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I will exercise extreme caution in connection with internet sites such as chatrooms, message boards and newsgroups and avoid inappropriate communication with individuals with whom I may be in a position of trust. This includes private use.
- I understand that I should not allow pupils or former pupils to become my 'friends' on social networking sites.
- I also understand that should I fail to follow the acceptable use policy the school may take action in line with the Disciplinary Policy.
- Complaints about cyber bullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to Child Protection are dealt with in accordance with school/local authority child protection procedures.