ADOPTED BY HCE : April 2018
REVIEWED: October 2019
DUE FOR ANNUAL REVIEW : October 2020

Online Safety and Acceptable Use of IT Policy

Contents

1. Rationale Page 3
2. Potential Online Safety Risks Page 3
3. Roles and Responsibilities Page 3
4. Online Safety in the Curriculum Page 4
5. Online Safety Support for Staff Page 4
6. Parental Involvement Page 5
7. The Internet Page 5
8. Online Communication and Collaboration Page 6
9. The Taking of Images and Film Page 8
10. Storage of Images Page 9
11. Personal Mobile Devices Page 9
12. Security Page 10
13. Incident Reporting Page 11
14. Viruses Page 11
15. Disposal of ICT Equipment Page 12
16. Decommissioned Accounts Page 12

Annex 1 - Acceptable Use Agreements

Annex 2 – Supporting Materials

1. Rationale

At Loughton, we interpret the term ‘information technology’ to include the use of any equipment which allows the users to communicate or manipulate information electronically. As a consequence, learning will be less dependent upon location and will take place 'anytime, anywhere' at the point of need. Online Safety encompasses the use of the internet and a range of new technologies, to create a safe working environment.

Online Safety, and related terms such as ‘online’, ‘communication technologies’ and ‘digital technologies’ refer to all fixed and mobile technologies that children may encounter, now and in the future, which might pose Online Safety risks (see Annex 2)

The internet and related technologies are becoming increasingly important in the daily lives of our children and have many positive benefits. They can be used both educationally and socially and are becoming part of a child’s identity. Socially our children often use the internet for entertainment, interaction, and communication with ‘friends’. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail and Instant Messaging Systems
- Social Media, including WordPress and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality, such as tablets, Kindles and Smart Watches
- Gaming platforms, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Video and Music Streaming

It is impossible to control access across all these devices in all situations where they might be used by children. However, if children can learn to become safe and discriminating users of technology, wherever and whenever they use it, they will be better placed to protect themselves against the risks and challenges they may encounter.

Children will experiment online and while their confidence and enthusiasm for using new technologies may be high, their understanding of the opportunities and risks may be low, alongside their ability to respond to any risks they encounter.

2. Potential Online Safety Risks

The Byron review classified Online Safety risks as involving **content, contact** and **conduct**. A child may be a recipient, participant or actor in online activities posing risk, as illustrated in the table below.

	Commercial	Aggressive	Sexual	Values
Content [child as recipient]	• Adverts • Spam • Sponsorship • Personal info • Inappropriate commercial advertising	• Violent/hateful content	• Pornographic / unwelcome sexual content	• Bias • Racist • Misleading information or advice • Radicalisation • Extremism
Contact [child as participant]	• Tracking online activity • Harvesting personal info. • Victim of a financial scam	• Being bullied, harassed, intimidated or stalked by an adult or child.	• Meeting strangers • Being groomed	• Self-harm • Unwelcome persuasions • Ideological persuasions from far right groups
Conduct [child as actor]	• Illegal downloading • Copyright infringement • Hacking • Gambling • Financial scams • Terrorism	• Bullying or harassing another • Anonymous 'trolling' or 'flaming' to others	• Creating and uploading inappropriate material • Sexual harassment	• Providing misleading information/advic e to peers • Reputation risk with publication of personal details

[Table developed by the EUKids Online project and referenced in paragraph 1.3 of the Byron Review]

The table illustrates that online safety risks are posed more by behaviours and values online than the technology itself. Rather than restricting access to technology, we need to empower learners to develop safe and responsible online behaviours to protect themselves whenever and wherever they go online. Children will experiment online and while their confidence and enthusiasm for using new technologies may be high, their understanding of the opportunities and risks may be low, alongside their ability to respond to any risks they encounter.

3. Roles and Responsibilities

At Loughton School, we understand the safeguarding responsibility to educate our pupils; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

As Online Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

This policy, supported by the school's Acceptable Use Agreements for staff, governors,

visitors, parents and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Safeguarding and Child Protection, Health and Safety, Behaviour (including the anti-bullying) and Personal, Social,

Health, Education and is read in conjunction with the Staff Code of Conduct and Social Media.

4. Online Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for Online Safety guidance to be given to the pupils on a regular and meaningful basis and so will ensure pupils have a broad and varied Online Safety curriculum.

Pupils are taught:

- about Online Safety throughout the curriculum.
- the online risks that they may encounter outside school.
- the relevant legislation when using the internet.
- about copyright, respecting other people's information and protecting their own personal information.
- the impact of Cyberbullying and are taught to seek help if they are affected by any form of online bullying.
- where to seek advice or help if they experience problems when using the internet and related technologies.
- the S.M.A.R.T rules (see Annex 2).
- to evaluate materials and learn good searching skills.

5. Online Safety Support for Staff

- Our staff receives regular and appropriate information and training on Online Safety and how they can promote the 'Stay Safe' online messages. They will have an annual refresher and staff meetings.
- New staff receive information and sign to say they adhere to and understand the school's Acceptable Use Agreement as part of their induction.-
- ***The DSL and Safeguarding Team have additional training to support them in the role (KCSIE2019)***

- All staff has been made aware of their individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community.

- All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas.

- All staff are encouraged to promote safe use of the internet and to promote children alerting an adult if they come across inappropriate content or are approached by someone online who may be a risk.

6. Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting Safety both inside and outside school and to be aware of their responsibilities. We regularly consult and discuss Online Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers and their child are asked to read through and sign Acceptable Use Agreements on behalf of their child on admission to the school. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. The Pupil Administration Manager will maintain this record.

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g. on school website).

- The school seeks to pass information to parents relating to Online Safety where appropriate in the form of:

    - Information and celebration evenings
    - Practical training sessions
    - Newsletter items
    - Alerts when specific issues are identified
    - Guidance in the website

7. The Internet

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

At Loughton School all use of the internet is logged and the logs are randomly but regularly monitored by the IT Manager, and overseen by the Headteacher. The IT manager and the headteacher have a good understanding of safeguarding issues as well as IT. Whenever any inappropriate use is detected it will be followed up with the

individual. Deliberate misuse may lead to disciplinary action being taken.

We ensure that our service provider is a member of the Internet Watch Foundation (IWF)

8. General:

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and wireless internet connectivity. Loughton Schools' internet access is controlled and filtered by E2BN's Equinet TINA Pilot Box.
- The school does not allow pupils access to internet logs.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- Online gambling or gaming is not allowed in school or using school equipment
- The use of unauthorised memory sticks/cards and flash drives is prohibited.
- Loughton School is aware of its responsibility when monitoring staff communication under current legislation.
- The school uses management control tools for controlling and monitoring workstations
- If staff or pupils discover an unsuitable site, the screen must be switched off and the incident reported immediately to the IT coordinator and the IT Manager. A log of the incident is taken, in the Online Safety log.
- It is the responsibility of the school, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- Pupils and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the IT Manager.
- The school does not allow any access to social networking sites for personal use in school time. Further guidance can be found in the Social Media Policy.

Staff:

- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- Good practice is that if internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. Furthermore, it is advised that parents recheck these sites and supervise this work. Ideally, parents will

be advised to supervise any further research.

- All staff, volunteers and governors must comply with the Social Media Policy regarding the posting of any information or images relating to the school.

- All staff are aware that deliberate or inadvertent access to inappropriate material must be reported to IT manager asap.

9. Online Communication and Collaboration

We recognise the range of communication tools available to our pupils and staff. This list includes blogs, email and social networking applications. We recognise that pupils and staff need to understand how to style correspondence in relation to audience, purpose and tone and have good network etiquette; 'netiquette'. Further guidance related to social networking can be found in the Social Media Policy.

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

- It is the responsibility of each account holder to keep the password secure. The school email and social media accounts should be used for all school business.

- Staff should not give their password to anyone else. Sharing passwords is a disciplinary offence.

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.

- Staff will be alert to children accessing materials that are offensive, derogatory or promote radicalisation.

- All e-mails and posts should be written and checked carefully by the author before sending, to ensure correct tone has been achieved for the intended audience.

- The forwarding of chain letters is not permitted in school.

- Online communication must not be used by any member of the school community to send or receive indecent or offensive images, videos or any written material of this kind. In addition, it should not be used by any member of the school community to cause intentional harm, upset, directly or indirectly to others.

<u>Pupils</u>

- Pupils may only use school approved accounts in school and with their teacher's guidance for educational purposes.

- Pupils may be given individual school issued accounts as well as use a class/ group e-mail address/ account.

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail/post whether directed at themselves or others and before it is deleted.

- Pupils are introduced to e-mail and appropriate, age related social networking as part of the Computing curriculum

- Pupils will notify their teacher if they access materials that are offensive, derogatory or promote radicalisation.

- Pupils should not use personal memory sticks/cards or flash drives on school computers.

- All pupils are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in communication or arranging to meet anyone without specific permission.

- Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting a child's work on the Internet, staff will ensure that permission has been given for work to be displayed. A list of those without consent will be stored centrally.

Staff should:

- ensure that their professional integrity is upheld when online.

- be aware that e-mails created or received as part of your school role will be subject to the Data Protection Act.

- Be aware that computers are regularly monitored for inappropriate activity, any breach will be followed up and may lead to disciplinary action.

- moderate posts/emails of pupils where possible.

- complete and Online Safety incident form if they receive an offensive e-mail/post whether it is directed at themselves or others and before it is deleted.

- be aware that school e-mail is not to be used for personal advertising.

- check their e-mail regularly.

- activate their 'out-of-office' notification when away for extended periods (only applies to Office Staff, SLG)

- open attachments from a trusted source only but should consult the IT Manager first if in doubt.

- not use the e-mail systems to store attachments related to pupils. Instead, they should detach and save business related work to the appropriate shared drive/folder.

10. Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

- Under no circumstances are staff, children or visitors permitted to use **personal** digital equipment, such as mobile phones and cameras, to record images of pupils, including when on field trips. This is to protect their integrity and reputation.

- Appropriate images can be taken only using school cameras; these should be transferred as soon as possible to the school's network, or hard drive of a staff laptop, and deleted from the individual device.

- Images taken in toilet/changing rooms are not allowed under any circumstances.

- Staff must have permission from parents/carers, before any image of the pupil can be uploaded for publication.

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

- Where an outside company or individual is commissioned by the school to take images, there must be appropriate DBS clearance and the school should satisfy itself that appropriate arrangements are in place to ensure images are not stored or distributed outside school.

- On certain occasions, for instance Sports Day and performances, parents and visitors may wish to take photographs or videos of groups of children. They will be reminded that these images and videos should not be uploaded to any Social Media or public website. If the school becomes aware of a breach in this advice, then the Headteacher will take action to ameliorate the situation.

11. Storage of Images

- Images/ films of children are stored on the school's network.

- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the permission of the Headteacher or IT Manager. These devices should have encryption capability.

- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource.

12. Personal Mobile Devices (including mobile phones)

Staff

- The school allows staff to bring in personal mobile phones and devices for their own use. Connection of any non-school owned equipment to the Wi-Fi service is not permitted.

- Personal mobiles should be locked away securely during the school day. Emergency calls must come in via school reception.

- Under no circumstances does the school allow a member of staff to contact children using their personal device, except in case of dire emergency. In such a case, the Headteacher should be informed.

- Staff should not contact parents/carers using their personal device without dialling 141 beforehand.

- The school is not responsible for the loss, damage or theft of any personal mobile device.

- The creation and sending of inappropriate or defamatory messages, images videos or sounds between any members of the school community is not allowed.

- Pupils

It is appreciated by the school that parents/carers would like their child to carry a mobile phone to and from school for safety reasons in Year 5 and 6. Pupils in Year 5 and 6 are allowed to bring their phones into school under the following conditions:-

- Phones are switched off before entering school and remain off until the pupil has left the school site.
- Phones are kept secure and locked away during the day.
- Phones are not used in school.

If a pupil fails to follow these conditions the pupil may be prevented from bringing the phone into school.

13. Security

The school gives relevant staff access to its Management Information System, with a unique username and password.

- It is the responsibility of everyone to keep passwords secure; these are not to be shared with others.

- Staff are aware of their responsibility when accessing school data

- Staff have been issued with the relevant guidance documents and have signed the

Acceptable Use Agreement

- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- All staff laptops are encrypted to secure school data (see Annex 2)
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under their control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed.
- All ICT equipment is security marked as soon as possible after it is received. The Office Admin Assistant, in liaison with the IT Manager, maintains a register of all ICT equipment and other portable assets.
- As a user of the school ICT equipment, staff are responsible for their activity.
- Staff are responsible for the backup and restoration of any of their data that is not held on the school's network.
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable devices. The local drive must be encrypted (see Annex 2 for encryption procedure)
- Computers should be locked in between use to avoid others accessing personal information.
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.
- Laptops must be shut down before transit to ensure they are in an encrypted state.
- Privately owned ICT equipment should not be used on a school network unless permission is granted prior by the Headteacher.
- On termination of employment, resignation or transfer, staff must return all ICT equipment to the school. Staff must also provide details of all their system logons so that they can be disabled.
- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- Equipment must be kept physically secure in accordance with this policy to be

covered for insurance purposes. When travelling by car, best practice is to place any laptop in the boot of the car before starting a journey.

- The installation of any applications or software packages must be authorised by the IT Manager

- Portable equipment must be transported in its protective bag.

- Anyone sending a confidential or sensitive fax should notify the receiver before it is sent.
  Confidential information being sent by email must be encrypted or password protected.

- There are regular checks undertaken on what children and staff are accessing on school equipment.

14. Incident Reporting

- All users are aware of the procedures for reporting accidental access to inappropriate materials or breaches of policy (see Annex 2).

- The incident log is used to monitor what is happening and identify trends or specific concerns. The log (see Annex 2) is kept in the school office.

- Any complaint about staff misuse (including sustained damage of equipment and other policy non-compliance) will be addressed by the Headteacher.

- In the case of the complaint being made in relation to the Headteacher, this will be referred to the Governing Body.

- Complaints of a child protection nature will be dealt with according to the Child Protection Policy and Safeguarding Policy.

- Online Safety incidents will be reported termly to the Governing body via the DSL.

- Any breaches of security involving data, must be reported to the IT Manager immediately who will follow the appropriate notification procedure.

15. Viruses

- We do not encourage the use of memory sticks or removable media, however this is sometimes essential any use must be authorised by the headteacher.

- The school has the right to check the content on any removable device used on school computers.

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-

virus software before being used.

- Anti-virus software installed on school ICT equipment will be untampered with.
- Personal provisional will be made to ensure computers/ devices not routinely connected to the school network, receive regular virus updates through the IT team.
- The IT manager must be notified of any suspected virus activity immediately, so that the necessary actions to remedy the situation can take place.

16. **Disposal of ICT Equipment**

- All redundant ICT equipment will be disposed of through an authorised agency recommended by the LA. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. If the storage media has failed it will be physically destroyed.
- Disposal of any ICT equipment will conform to current legislation and will conform with the governors' policy on the disposal of equipment.

17. Decommissioned Accounts

- The office staff will notify the IT manager of children/staff who are leaving. The IT Manager will ensure that all user accounts are disabled once that member of the school has left the school, so that internal security remains robust and uncompromised.
- Accounts to any school social networking applications and other online learning tools will be decommissioned once that member of the school has left the school, to prevent conflicting accounts.
- Criminal use of Internet or Accessing Illegal materials
- Anyone found to be using the school internet for criminal activity or using the school system to access illegal materials will be reported to the Police.