Tower Hill Primary School
e-Safety Policy

Date: Autumn 2019 **Reviewed:** Laura Ovenden
Next Review Date: Autumn 2020 Headteacher

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Tower Hill Primary School with respect to the use of ICT-based technologies.
- safeguard and protect all children and staff.
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

Scope

This policy applies to all members of Tower Hill Primary School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Tower Hill Primary School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular monitoring reports from the e-Safety Co-ordinator • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager)
e-Safety Coordinator / ICT Leader	• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents • promotes an awareness and commitment to e-safeguarding throughout the school community • ensures that e-safety education is embedded across the curriculum • oversees the delivery of the e-safety element of the Computing Curriculum • liaises with school ICT technical staff • communicates regularly with SLT and the designated e-safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs • ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • ensures that an e-safety incident log is kept up to date

Role	Key Responsibilities

	• facilitates training and advice for all staff
	• liaises with the Local Authority and relevant agencies
	• is regularly updated in e-safety issues and legislation, and is 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 and use of social media

Governors / e-Safety Governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the e-Safety Policy and review the effectiveness of the policy. This will be carried out by the nominated governor for e-safety who will receive regular information about e-safety incidents and monitoring reports and report back to the Full Governing Body. To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the e-Safety Governor will include: • regular review with the e-Safety Co-ordinator / Officer (including e-safety incident logs, filtering / change control logs)
Network Manager/ Technician (Harrap IT)	• To report any e-safety related issues that arise, to the e-Safety Co-ordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced Password Protection Policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • that he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-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 e-Safety Co-ordinator / Headteacher for investigation • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures

Role	Key Responsibilities
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use of ICT Policy • To be aware of e-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 • To report any suspected misuse or problem to the e-Safety Co-ordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use of ICT agreement (NB: at KSI it would be expected that parents / carers would sign on behalf of the pupils). • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • understand the importance of reporting abuse, misuse or access to inappropriate materials. • know what action to take if they or someone they know feels worried or vulnerable when using online technology. • know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • know and understand school policy on the taking / use of images and on cyber-bullying. • understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school. • take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home.

Role	Key Responsibilities
	• help the school in the creation/ review of e-safety policies
Parents/carers	• to support the school in promoting e-safety • to read, understand and promote the school Pupil Acceptable Use of ICT agreement with their children • to access the school website in accordance with the relevant school Acceptable Use Agreement. • to consult with the school if they have any concerns about their children's use of technology

Communication:
The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be available on the school website and staffroom
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and ICT file

Handling Complaints:

- 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 or 1:1 teaching by the eSafety Co-ordinator or Headteacher;
  - informing parents or carers;
  - removal of Internet or computer access for a period;
  - referral to LA / police.

- Our e-Safety Co-ordinator 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 within the school's Behaviour Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Education and Curriculum

Pupil e-Safety Curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing Curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - to STOP and THINK before they CLICK
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
    - [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
    - to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying;
    - to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use of ICT agreement which every student will sign.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- 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 respect and acknowledge 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.

Staff and Governor Training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues and the school's e-safety education program;
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on this e-Safety Policy, the Data Protection Policy and the school's Acceptable Use of ICT Policies.

Parent Awareness and Training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear;
    - suggestions for safe Internet use at home.

Expected Conduct and Incident Management

Expected Conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use of ICT Policy which they will be expected to sign before being given access to school systems (at KSI it would be expected that parents/carers would sign on behalf of the pupils);
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school;
- 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.

Staff

- are responsible for reading the school's e-Safety Policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-Safety Acceptable Use of ICT agreement form at time of their child's entry to the school;
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident Management

In this school:

- there is strict monitoring and application of the e-Safety Policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions;
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (e.g. the Local Authority, UK Safer Internet Centre Helpline) in dealing with e-safety issues;
- monitoring and reporting of e-safety incidents takes place and contribute to developments in policy and practice in e-safety within the school;
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible;
- we will contact the police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

Managing the ICT Infrastructure

To ensure the network is used safely, this school:

- ensures staff read and sign that they have understood the school's e-Safety Policy. Access to the shared network is through a unique, audited username and password. We also use the same username and password for access to our remote network;
- makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- 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;
- where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
- 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; e.g. equipment installed and checked by approved suppliers / LA electrical engineers;
- ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems;
- does not allow any outside agencies to access our network remotely;
- makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external audit's requirements;

- installs all computer equipment professionally and meets health and safety standards;
- maintains projectors so that the quality of presentation remains high;
- reviews the school ICT systems regularly with regard to health and safety and security.

Password Policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

Please read this in conjunction with the school's Password Policy.

E-mail

This School

- Does not publish personal e-mail addresses of pupils or staff on the school website.
- Will contact the police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the police.

Pupils:

- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
    - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
    - that an e-mail is a form of publishing where the message should be clear, short and concise;
    - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
    - that they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - that they should think carefully before sending any attachments;
    - that embedding adverts is not allowed;
    - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
    - not to respond to malicious or threatening messages;
    - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
    - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
    - that forwarding 'chain' e-mail letters is not permitted.

Staff:

- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
    - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
    - the sending of chain letters is not permitted;
    - embedding adverts is not allowed.

School Website

- The ICT Leader takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers: The ICT Leader, Senior Leadership Team and users approved for authorisation by the Head Teacher
- The school web site complies with the statutory DfE 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, telephone number and we use a general email contact address, e.g. info@schooladdress or admin@schooladdress. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' full names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images.

Social Networking

School staff will ensure that in private use:

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

Digital Images and Video

In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs.
- Staff sign the school's Acceptable Use of ICT Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.

- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use.
- The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

For more information about Tower Hill Primary School's use of the Internet and Digital Equipment please also read the:

- Data Protection Policy
- Internet Access and Acceptable Use of ICT Policy
- Pupil Acceptable Use of ICT Agreement
- Social Media Policy