E-Safety Policy

CIT Strategic Lead of Technology - Tom Booth
Online Safety Officer– Luke Allen
Headteacher – Tina Cox

Introduction to Online Safety at Tulip Academy Spalding
This policy must be read in conjunction with Lincolnshire Safeguarding Children's Board Interagency Procedures. These procedures can be accessed via the LCSP website: https://www.lincolnshire.gov.uk/safeguarding/lscp.

The school has a duty to ensure that safeguarding permeates all activities and functions. This policy therefore complements and supports a range of other Tulip Academy Spalding and CIT policies, for instance:

- Child Protection & Safeguarding
- Anti-Bullying
- Staff Handbook and Code of Conduct
- Special Educational Needs, including the Local Offer
- Health and Safety
- Sex and Relationships Education
- Parenting Contract and Home/School Agreement Policy
- Curriculum
- Acceptable use of the Internet & IT Systems
- Data Protection
- Photography & Social Media
- Mobile Phone
- Child Sexual Exploitation

The Designated Safeguarding Lead will act as the Online Safety Officer in relation to their role as it does not require technical expertise. The Computing Subject Leader will also support the team and their duties, linked to this role. In conjunction with ARK Solutions and the CIT Strategic Lead of Technology, they will monitor the use of the internet and other digital technologies used in the school.

Our Vision
CIT encourages use by pupils of the rich information resources available on the internet, together with the development of appropriate skills to analyse and evaluate such resources.

At Tulip Academy Spalding, we celebrate all individuals, organisations and cultures and foster trust and respect to prepare our learners for the next stages in their lives. We recognise that the technology plays an important part in supporting a pupil's ability to

learn and become prepared in the 21st Century. We therefore aim to provide an education that provides pupils with opportunities to explore and develop their use of technology, how to stay safe on various technological devices, what support is available to our pupils and their families and how to protect their digital footprint.

Whole School Responsibilities

Local School Board (LSB)
The LSB is accountable for ensuring that our school has effective policies and procedures in place. Their outlined duties and responsibilities are:

- To review this policy at least annually and in response to an online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school.
- To ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- To provide appropriate challenge and support to senior leaders and the staff team.
- To become updated with emerging risks and threats through technology use. The governor in charge of CPD and/or the Clerk is to identify appropriate training and consultancy to ensure they are updated.
- To receive regular updates from the Senior Leadership Team or Designated Safeguarding Lead during meetings, monitoring visits and Safeguarding Learning Walks.
- To appoint an LSB member, who will monitor and evaluate online safety within the school.
- To promote online safety systems and processes to parents, carers and the wider community.

The Headteacher and Leadership Team

The Headteacher and Leadership Team are to ensure that the school has effective policies and procedures in place. In accordance to their outlined duties and responsibilities, they are:

- To ensure that there is adequate online safety training throughout the school and that it is planned, efficient, relevant and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- To ensure that the Safeguarding Team have had appropriate CPD in order to undertake the day to day duties.
- Monitoring and evaluating the appropriateness and impact of how we record online safety incidents.
- To ensure that all online safety incidents are dealt with promptly and appropriately.

- Ensure that the Online Safety Officer is given time, support and authority to carry out their duties effectively
- Ensure the Online Safety Officer is kept informed of development at Local Authority level.
- Ensure that the Governing body are kept informed of online safety issues.

The Designated Online Safety Officer

Their primary responsibility is to establish and maintain a safe learning environment ensuring online safety rules are displayed in school. In accordance to their outlined duties and responsibilities, they are:

- To ensure that the individual is updated and is aware of the latest risks to pupils, whilst using technology. This includes becoming familiar with the latest research and available resources for school and home use.
- To advise the governing body on all online safety matters.
- To engage with parents, carers and the school community on online safety matters at school and/or at home.
- To liaise with the Local Authority, CIT Trust, technical support and other agencies as required.
- To retain responsibility for the online safety incident log.
- To ensure staff know what to report, how to report this and ensure the appropriate documentation is completed.
- To ensure any technical online safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ARK Technical Support.
- To liaise with the Headteacher and responsible LSB member to decide on what reports may be appropriate for viewing.
- To liaise and work alongside the Computing Subject Leader, PSHE/SMSC/RSE Leader and the Senior Leader with responsibility of Curriculum to establish, maintain and review, when necessary, a school-wide online safety programme.
- To be responsible for ensuring staff are confident to deliver online safety lessons.
- To monitor, review and evaluate online safety policies and procedures.

Technical Staff (ARK Technical Solutions):

Technical support staff are responsible for ensuring that the Tulip Academy Spalding infrastructure is secure; this will include at a minimum:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows and Apple updates are regularly monitored and devices updated as appropriate.
- Any online safety technical solutions such as Internet filtering are operating correctly.

- Filtering levels are applied appropriately and according to the age of the user. This also includes that categories of use are discussed and agreed with the Online Safety Officer and Leadership Team.
- Every child and every member of staff will have an individual username and password.

In addition to ensuring the infrastructure is secure, they are expected:

- To ensure that appropriate processes and procedures are in place for responding to the discovery of illegal materials, or suspicion that such materials are, on the school's network.
- To ensure that appropriate processes and procedures are in place for responding to the discovery of inappropriate but legal materials on the school's network.
- To maintain an understanding of relevant legislation.
- To report network breaches of acceptable use of ICT facilities to the CIT Strategic Lead of Technology, Tulip Academy Spalding Online Safety Officer and the Headteacher.
- To maintain a professional level of conduct in their personal use of technology, both within and outside school.
- To take responsibility for their own professional development.

School Staff:

The staff are to ensure that the school are adhering to processes, policy and procedures in place. In accordance to their outlined duties and responsibilities, they are:

- To become familiar with information within this policy and that this is understood. If anything is not understood, it should be brought to the attention of the Headteacher or Designated Safeguarding Lead.
- To adhere to the CIT Code of Conduct, Acceptable Use of Internet and relevant policies about technology, prior to using school IT equipment.
- To take responsibility for the security of data in accordance to General Data Protection Regulations (GDPR).
- To model good practice in using new and emerging technologies.
- To maintain an awareness of online safety issues, and how they relate to pupils in their care.
- To address online safety concerns that arise as a result of gaming or social media, in or outside of school, and report these to the Online Safety Officer or the Headteacher, in their absence.
- To embed and incorporate online safety education in the delivery of the curriculum.
- To know when and how to escalate online safety issues.

- To maintain a professional level of conduct in their personal use of technology, both within and outside school.
- To report any virus outbreaks to ARK Technical Solutions, the CIT Strategic Lead of Technology and the Online Safety Officers who will, in turn, inform the relevant Local Authority Helpdesk as soon as it is practical to do so.
- To become aware that the school network and internet traffic is monitored, both at school and Local Authority level and can be traced to an individual user. Discretion and professional conduct are imperative at all times.

Volunteers, Students and Trainee Teachers:

Any person not directly employed by the school will be asked to attend a Safeguarding Induction, where they will be outlined information appropriate to the school and safeguarding protocol before being allowed to access the internet from the school site.

Pupils:

The pupils are to ensure that they are adhering to processes, policy and procedures in place. In accordance with this, they are:

- To be informed that network and Internet use will be monitored.
- To be informed that any deviation or misuse of technology or services will be reported to the relevant individuals and the behaviour policy will be followed.
- To hand in technological devices, using the school's implemented system, for safe keeping. Any necessary phone calls and communication will be made by school staff.
- To engage and become aware of advice and guidance available to ensure they are safe online and that their digital footprint is protected from others.
- To adhere and follow all examination rules and regulations, regarding their use of technology.

Parents, Carers and the Wider Community:

Parents, carers and their communities play an important role in their child's development and due to this, the school will ensure that they have the knowledge and skills to promote good online safety practice and how they can maintain high levels of safety outside the school environment. The school will ensure that they communicate:

- Through newsletters, ParentMail, the offer of workshops and the Tulip Academy Spalding website the school will draw attention to the school Online Safety Policy and keep them up to date with new and emerging online safety risks.
- When appropriate, the school will inform parents of online safety concerns regarding online gaming and social media and signpost parents to websites and articles which offer practical advice.

- Upon induction and admission processes, the school will notify families of our procedures, to ensure that they are properly safeguarding. All parents must consent to confirm:
- Whether or not images, videos and names may be used for school purposes including the school website, social media platforms and local publications. Non-return of the permission slip will not be assumed as acceptance.
- Individual permission may be sought from parents if their child is attending an event outside school (e.g. – music and sports events at other schools where photographs/video may be taken and used for promotional purposes.)

Technology at Tulip Academy Spalding:

Tulip Academy Spalding uses a range of devices including PC's, laptops, Apple Macs, iPads, Kindles and personalised devices for specific pupils, upon advice from professionals. In order to safeguard the pupil and in order to prevent loss of personal data we employ the following assistive technology:

- Internet and Email Filtering – Senso.cloud technology is utilised in school and we work alongside ARK Technical Solutions to prevent unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Computing Leader, Online Safety Officer and Technical Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher or Deputy Headteacher.
- Anti-Virus Systems – All capable devices will have anti-virus software. This software will be updated regularly for new virus definitions. Technical Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.
- Data Protection - All sensitive or confidential information is stored/transferred with reference to the Data Protection Act and in accordance with the Acceptable Use of Internet policy and the CIT Data Protection Policy.

The School Website

The Headteacher, or designated staff member, will take overall editorial responsibility and ensure that content is accurate and appropriate. They will ensure that:

- Staff or pupil personal contact information will not be published.
- Photographs/videos that include pupils will be selected carefully so that their image cannot be misused. Pupils' photographs/videos will only be used if consent has been given by their parent or carer. Full names will not be used anywhere on the school website in association with photographs/videos.
- All uploaded data conforms to copyright law.
- If it should come to the school's attention that there is a resource that has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed.

Social Media and Networking Sites

There are many social networking services available and Tulip Academy Spalding is fully supportive of social networking as a tool to engage and collaborate pupils, families and the wider school community. The following social media services are permitted for use within Tulip Academy Spalding and have been appropriately risk assessed.

- Twitter and Facebook - The Tulip Academy Spalding Twitter and Facebook accounts will be a public account which will run alongside more traditional methods of communication not replace them. This will be monitored by an administrator, who will report incidents, if deemed necessary to the Online Safety Officer or the Headteacher.

Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and will be reviewed by the senior leadership team. In addition to this, should staff wish to use other social media, permission must first be sought via the Online Safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

Safeguarding

Cyber-crime and online safety are embedded in the Digital Literacy strand, within our Computing curriculum. For example, pupils learn about hacking, cyberbullying and malware attacks. In addition, and where appropriate, discussions will be had about the Computer Misuse Act and the importance of this in school and the future workplace. Our role at Tulip Academy Spalding is to ensure pupils are prepared for life after school and understand the risk of cyber-crime. By sharing strategies and techniques in high-quality teaching, this allows pupils to make informed choices and apply their cyber skills.

Child Criminal Exploitation of children is a geographically widespread form of harm that affects children both in a physical and virtual environment. Organised criminal groups or individuals exploit children and young people due to their computer skills and knowledge. Their ability allows criminals to access networks, data and information which is used for criminal or financial gain. If a member of school staff is concerned that a pupil is engaged in cyber-crime, they should contact the Designated Safeguarding Lead, or deputy in their absence to discuss their concerns.

In addition to this, a referral can be made to East Midlands Cyber Secure Services: www.eastmidlandscybersecure.co.uk by anybody. This platform is to share concerns about a child and their cyber behaviours. They work closely with a range of children's services across the East Midlands. Once a referral is made, they gather and de-conflict information relating to the referral. They contact the family about the referral and when appropriate, a visit will be made to complete an assessment of knowledge, skills and vulnerability. Once complete, further support will be provided to continue multi-agency support.

East Midlands Cyber Secure Services also offer support to families, staff and agencies with resources and assemblies to further educate children and young people with cyber-crime and online safety.

Assessing Risks & Reporting Incidents

Any online safety incident is to be brought to the immediate attention of the Online Safety Officer, or in his/her absence the Headteacher. The Online Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log. All incidents, alleging illegal or inappropriate activity, will be dealt with in accordance with the school child protection procedures. Whilst our Trust promotes the use of technology and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that technology is used appropriately. Any misuse of technology will not be taken lightly and will be reported to the Headteacher, or Trust IT Lead in order for any necessary further action to be taken.

Any appropriate risk assessments will be implemented by the Online Safety Officer in liaison with the Health & Safety Officer (the senior leadership team in their absence) and ARK Technical Solutions. Assessments will be monitored and reviewed regularly and when the need arises.

The online safety policy will be regularly reviewed to ensure that it is adequate, appropriate and effective. The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computational device connected to the school network. Neither the school nor CIT Academies can accept liability for any material accessed, or any consequences of internet access.