Behaviour & Attitudes

E-Safety Policy

October 2023

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 Greenfields 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 the 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.

Greenfields Academy

At Greenfields 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 a 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 Senior Leadership Team

The Headteacher and Senior 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 subject champions and the Assistant Headteacher 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 Greenfields 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, Greenfields 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.

Greenfields 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 DSL
- 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.

Greenfields Pupils:

The pupils are to ensure that they are adhering to processes, policy and procedures in place. In accordance to 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.
- To follow the principles of the 1:1 Pupil Technology Device & Acceptable Use Agreement (Appendix 1)

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, Social Media posts,Teachers2Parents or email the offer of workshops and the Greenfields 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.)
- Parents will support their child to read, understand and follow the principles of the 1:1 Pupil Technology Device & Acceptable Use Agreement (Appendix 1)

Technology at Greenfields

Greenfields 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 – 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 School Leader in Charge. Filtering and monitoring standards are embedded as set out in the CIT Statement for the meeting of DfE Filtering and Monitoring Standards (Appendix 2)
- 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 Greenfields 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 Greenfields and have been appropriately risk assessed.

• Twitter and Facebook - The Greenfields 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 Greenfields 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 cybercrime and online safety. The East Midlands Cyber Protect Network is coordinated by the East Midlands Special Operations Unit (EMSOU) and can be contacted via telephone or email:

- Telephone: 0300 123 2050 or in an emergency, dial 999 or 112.
- Email: cybercrime@lincs.pnn.police.uk

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, Designated Online Safety Officer 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.

Policy Review

Greenfields considers the Online Policy document to be important. The Leadership Team will undertake a thorough review of both policy and practice each year and report to the Local School Board annually

Policy produced: October 2022

Reviewed: October 2023

Next Review: October 2024

Appendix 1: 1:1 Pupil Technology Device & Acceptable Use Agreement

Beginning with the 2023/24 school year, Greenfields Academy will provide each student a device (i.e., a laptop), which the student is to use as a positive learning tool in coordination with the academy's curriculum. Although this agreement authorises the pupils' use of the device for the year, the device is the property of the academy and must be returned upon the academy's request or on the last day of the student's attendance for the school year.

This Agreement is entered into between Greenfields Academy, the Pupil and the Parent(s)/Guardian(s) of the Pupil. To receive a device to use, the student must have an attendance of at least 80% and the student and his or her parent/guardian must sign and submit to this 1:1 Student Technology Device & Acceptable Use Agreement.

Greenfields Academy understands the benefits technology can have on enhancing the curriculum and pupils' learning; however, we must ensure that pupils respect school property and use technology appropriately. To achieve this, we have created this acceptable use agreement which outlines our expectations of pupils when using technology, whether this is on personal or school devices and on or off the school premises. Please read this document carefully and sign below to accept that you agree to the terms outlined.

Using technology in school

- I will only use ICT systems, e.g., computers, laptops and tablets, which my class teacher has given me permission to use.
- I will only use approved school accounts (email etc.) provided to me by the ICT technician.
- I will not store or use any personal data relating to a pupil or staff member for non-school related activities. If I have any queries about storing or using personal data, I will speak to my class teacher.
- I will delete any chain letters, spam, and other emails from unknown senders without opening them.
- I will ensure that I get permission from my class teacher before accessing learning materials, e.g., source documents, from unapproved sources.
- I will only use the internet for personal use during out-of-school hours, including break and lunchtimes. During school hours, I will use the internet for school work only.
- I will not share my passwords, e.g., to my school email account, with anyone.
- I will not install any software onto school ICT systems unless instructed to do so by my class teacher.
- I will only use recommended removable media, e.g., encrypted USB drives, and I will keep all school-related information stored on these secure.
- I will participate fully in E-Safety lessons and adhere to the online safety guidelines I have been taught.
- I will only use the school's ICT facilities to: - Complete homework and coursework. - Prepare for lessons and exams. - Undertake revision and research. - Gather or process information for extracurricular activities, e.g., creating the school newsletter.
- I will not use the school's ICT facilities to access, download, upload, send, receive, view or display any of the following: - Illegal material - Any content that could constitute a threat, bullying or harassment, or anything negative about other persons or the school - Content relating to a person's sexual orientation, gender, religion, race, disability or age - Online gambling - Content which may adversely affect the reputation of any organisation (including the school) or person, whether or not they are known to be true or false - Any sexually explicit content - Any personal data or information.

Mobile devices

- I will use school-owned mobile devices, e.g., laptops and tablets, for educational purposes only.
- I will seek permission from my class teacher before a school-owned mobile device is used to take images or recordings.
- I will not use any mobile devices to take pictures of fellow pupils unless I have their consent.
- I will not use any mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.

- I will not access the Wi-Fi system using personal mobile devices unless permission has been given by my class teacher or the ICT technician.
- I will not take or store images or videos of staff members on any mobile device, regardless of whether it is school-owned.

Social media

- I will not use any school-owned mobile devices to access personal social networking platforms.
- I will not communicate or attempt to communicate with any staff member over personal social networking platforms.
- I will not accept or send 'friend' or 'follow' requests from or to any staff member over personal social networking platforms.
- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the school on any social networking platforms which may affect the school's reputation.
- I will not post or upload any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- I will not post any material online that: - Is offensive. - Is private or sensitive. - Infringes copyright laws. - Damages the school's reputation. - Is an image or video of any staff member, parent or nonconsenting pupil.

Reporting misuse

- I will ensure that I report any misuse or breaches of this agreement to the class teacher or headteacher.
- I understand that my use of the internet will be monitored by the IT Technical staff and recognise the consequences if I breach the terms of this agreement.
- I understand that the headteacher may decide to take disciplinary action against me in accordance with the school's Policy if I breach this agreement.

I have read and understood this agreement and will ensure that I will follow by each principle.

Name of Pupil:	
Signed:	
Date:	

I have read and discussed with my child the 1:1 Pupil Technology Device & Acceptable Use Agreement for school and understand that will help keep my child safe online. I am aware that the use of school devices and systems may be monitored for safety and security reason to keep my child safe. This monitoring will take place in accordance with data protection, privacy, and human rights legislation.

Name of Pupil:	
Name of Parent:	
Signed:	
Date:	

Appendix 2: CIT Statement for the meeting of DfE Filtering and Monitoring Standards

C.I.T
Where learning comes first

CIT Statement for the meeting of DfE Filtering and Monitoring Standards:

Technical information:

The trust has implemented SENSO as the chosen monitoring software.

Filtering system is called 'Securly'

SENSO is on the DFE directory of UK SENSO is configured to send an email including a screen shot and user details to the DSL if a student access inappropriate content. The DSL will the investigate and resolve appropriately. The IT staff will be notified to action an immediate internet ban and blockage of websites Safety Tech Providers.

IT Lead is responsible for maintaining the effectiveness of filtering and monitoring systems across the Trust. The Lead IT is responsible for the procurement of the filtering and monitoring across the trust and meets regularly with the IT support company and the filtering company to ensure inappropriate sites are blocked.

Strategic Information:

Internet filtering and monitoring comes under the overarching umbrella of safeguarding and as such is the responsibility of the DSL to assure effectiveness.

Governing bodies and proprietors have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met.
At CIT, governance sits with our Trust Board.

Our board have delegated a series of assurances to local school boards – LSBs to provide information to the board via regular reporting systems.

Safeguarding is one of the LSB delegated assurances.

The operational effectiveness of internet filtering and monitoring PLUS the consistency of response from staff and pupils to breaches in individual schools is part of the assurance from the LSB to the Trust Board.

The strategic accountability for the effectiveness of the filtering and monitoring systems sits with the Trust Board.

The Trust has provided a document for all schools (see attached) that shows how we meet the required standards.

Our systems and procedures are reviewed annually by our central IT team. This is informed by information contained in LSB and headteacher assurances. LSBs will share this information through their regular existing reporting arrangements under the umbrella of their Safeguarding information.

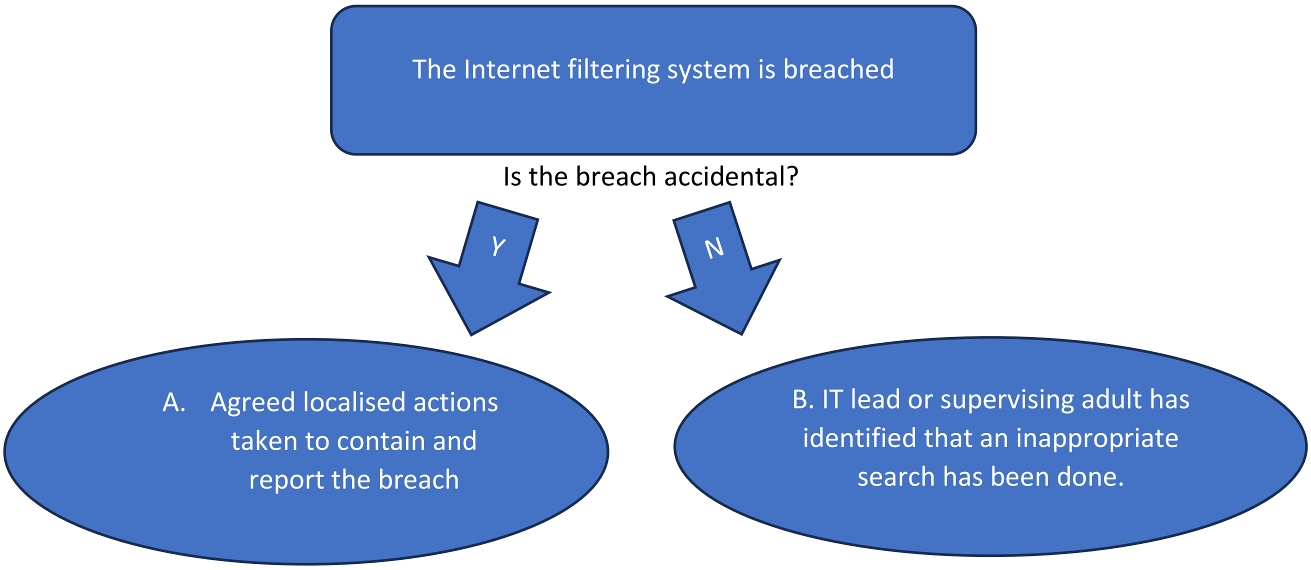
Schools will have a consistent, rapid localised response to the strategy they adopt when firewalls and filters are breached by inappropriate content. All staff and pupils must be aware of this process and can verbalise it clearly as well as use it.

This should include:

- How other children are protected from seeing inappropriate images i.e., they know to immediately close the laptop or turn the screen off.
- How they make sure an adult knows they have seen something that makes them feel uncomfortable (learning about what is appropriate and what is not, should be part of the E-Safety curriculum)
- What adults then do with that information.

Any accidental breaches of the filtering system MUST be noted and passed on to the DSL who will ensure the IT team at the centre are aware. How the school chooses to do this is decided by SLT and LSB.

The central IT team will block any sites or content that are reported by schools.



The Internet filtering system is breached

Is the breach accidental?

A. Agreed localised actions taken to contain and report the breach

B. IT lead or supervising adult has identified that an inappropriate search has been done.

	A	B
Subsequent actions to be taken by leaders:	Written report received from supervising teacher containign the information what, when and by whom. DSL to contact IT to let them know what has got through. IT team will take action to remove and block.	MIS (CPoms/Schoolpod) report to DSL to show what who, what, when. DSL to take appropriate investaigatory activities accordign to policy. If the search has been identified by the IT lead at centre, the school must be informed and the DSL to investigate and take the appropriate action to safeguard the individuals