Leadership & Management

Online Safety Policy

Contents	
1	Policy Intent
2	Roles & Responsibilities
3	Responding to Online Abuse
4	E-Safety Education
5	Assessing Risks & Reporting Incidents
6	Technical – Infrastructure and equipment filtering and monitoring
7	Use of digital and video images
8	Data Protection
9	Communications
10	Links to other policies
11	Review
12	Appendices

1.0 Policy Intent

Computing and the use of digital devices is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. At Greenfields Academy we understand the responsibility to educate our pupils on e-safety issues, 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.

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

The Education and Inspections Act 2006 empower 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 sanctions for inappropriate behaviour. This is relevant to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. The school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

The aim of this policy is to:

- Ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices.
- Provide staff and volunteers with the overarching principles that guide our approach to online safety.
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices

The policy applies to all staff, volunteers, children and young people and anyone involved in Greenfield's activities.

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Monitoring logs of internet activity (including sites visited)/filtering.
- Internal monitoring data for network activity.

2.0 Roles & Responsibilities

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. The named Safeguarding Governor will be responsible for overseeing the online safety procedures of the school. This will include:

- Regular meetings with the Computing Subject Lead.
- Regular monitoring of online safety incident logs.
- Regular monitoring of filtering/change control logs.
- Reporting to relevant Governor's meeting.

Headteacher

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Headteacher and Senior Leaders are responsible for ensuring that the Computing Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will work with ARK, who provide IT monitoring and filtering systems across the school's electronic devices and receive reports of any monitoring concerns.

Designated Safeguarding Lead

The Designated Safeguarding Lead will act as the Online Safety Officer in relation to their role as it does not require technical expertise. Their primary responsibility is to establish and maintain a safe learning environment ensuring online safety rules are displayed in school. In accordance with 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 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 Support

The school receive technical support from ARK who are responsible for implementing relevant filters to all electronic devices. They will ensure:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any MAT online safety policy/guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the networks, internet and digital technologies are regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher for investigation and necessary action.
- That monitoring systems are implemented and updated as agreed in policies.

Computing Subject Leader

The identified Computing Subject Leader will:

- Have a clear understanding about the nature of computing as a subject and learning medium
- Disseminate resources and training developments throughout the staff team
- Monitor and review the computing provision across the school
- Support staff development in the use of computing across all subjects
- Support the Online Safety Officer in their duties and role.

Teaching and support staff

- Have an up-to-date awareness of online safety matters and of the current school online safety policy and practices.
- They have read, understood the CIT Acceptable Use of the Internet policy.
- They report any suspected misuse or problem to the headteacher or designated safeguarding lead for investigation.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the Online Safety Policy.
- They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches and not blocked by the current filtering system.
- Report any inappropriate websites that are not blocked through the filtering system to ARK.

Pupils

- Are responsible for using the school digital technology systems in accordance school policies.
- 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 online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' meetings, newsletters, letters, website, social media and information about national and local online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice.

3.0 Responding to Online Abuse

If online abuse occurs, we will respond to it by:

- Having clear and robust safeguarding procedures in place for responding to abuse (including online abuse).
- Providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation.
- Making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account.
- Reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

4.0 E-Safety Education

Pupils

Whilst technical solutions are very important, pupils use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is incorporated in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum will be provided in the following ways:

- A planned online safety curriculum is provided as part of Digital Citizenship, Computing, and PSHE.
- Key online safety messages are reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils should be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be encouraged to understand the need to adopt safe and responsible use of the internet both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Parents/Carers

Parents and carers play an essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities.
- Letters, newsletters, web site.

- Parents/carers evenings/sessions.
- High profile campaigns e.g. Safer Internet Day.
- Reference to the relevant web sites/publications.

Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.

5.0 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 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.

Cyber-bullying

Cyber-bullying can be defined as the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages; the size of the audience; perceived anonymity; and even the profile of the person doing the bullying and their target.

Cyber-bulling can have a serious effect on pupils both in and outside school. The methods and the audience are broader than traditional bullying and the perceived anonymity can make escalation and un-intended involvement an increased risk. Greenfields Academy has a range of strategies and policies to prevent online bullying, outlined in various sections of this Policy.

These include:

- No access to public chatrooms, Instant Messaging services and bulletin boards.
- Pupils are taught how to use the Internet safely and responsibly and are given access to guidance and support resources from a variety of sources.
- Pupils are encouraged to discuss any concerns or worries they have about online bullying and harassment with staff, who have a range of materials available to support pupils and their families.
- Pupils are informed on how to report cyber bullying both directly within the platform they are on, and to school.
- Complaints of cyber bullying are dealt with in accordance with our Anti-bullying Policy.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.

Grooming

Grooming is a word used to describe how people who want to co-opt or potentially harm children and young people get close to them, and often their families, and gain their trust. Online grooming may occur by people forming relationships with children and pretending to be their friend. They do this by finding out information and seeking to establish false trust. The school has measures in place to educate and protect pupils against this risk. These include:

- No access to public chatrooms, Instant Messaging services and bulletin boards. No mobile phones.
- All online access and pupil generated content in school is monitored and password protected.
- Pupils are taught how to behave responsibly online and the 'golden rules' in protecting personal information.
- Pupils, staff, parents and governors are provided with appropriately targeted training on risks and solutions to keep safe online.

Cyber Crime

Cybercrime is an umbrella term used to describe two closely linked, but distinct ranges of criminal activity. These are defined as:

- Cyber-dependent crimes - Crimes that can be committed only through the use of Information and Communications Technology ('ICT') devices, where the devices are both the tool for committing the crime, and the target of the crime. For example: developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity.
- Cyber-enabled crimes – Traditional crime that is enhanced in scale or reach by use of technology. For example: cyberbullying, online fraud, online grooming, malicious communications.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority.
- Obtain unauthorised access to a computer.
- "Eavesdrop" on a computer.
- Make unauthorised use of computer time or facilities.
- Maliciously corrupt or erase data or programs.
- Deny access to authorised users.

If a pupil or staff member comprises the school's network or commits a Computer Misuse Act offence against the school or anyone inside the school using high level computer skills a referral will be made to the East Midlands Special Operations Unit Cyber Prevent Team. See www.cyber4schools.net for more information.

6.0 Technical – Infrastructure and equipment filtering and monitoring

The school will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider. Content lists are regularly updated, and internet use is logged and regularly monitored.
- Internet filtering and monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided differentiated user-level filtering.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data.

- An agreed policy is in place regarding the extent of personal use that users (staff/students/pupils) and their family members are allowed on school devices that may be used out of school;

7.0 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital and video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' photographs will not be taken without the consent of the pupil.

8.0 Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. See CIT Data Protection policy for more information.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- Can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school.
- Will not transfer any school/academy personal data to personal devices except as in line with school policy.
- Access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged off" at the end of any session in which they are using personal data.

9.0 Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the school/academy considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users should be aware that email communications are monitored.
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

10.0 Links to other policies
This policy complements and supports a range of other policies, for instance: • Child Protection policy • Behaviour policy • Anti-bullying policy • CIT – Acceptable Use of Internet policy • CIT – Code of Conduct • CIT – Data Protection Policy • CIT – Mobile Device Policy • CIT – Photography Social Media policy • CIT – Code of Conduct – Parent and Carer

11.0 Review
Date Written: December 2024 Last Review: December 2025 Next Review Date: December 2026

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

Greenfields Academy provide each pupil with devices (i.e., a laptop), which the student is to use as a positive learning tool in coordination with the academy's curriculum.

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 schoolwork 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

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.

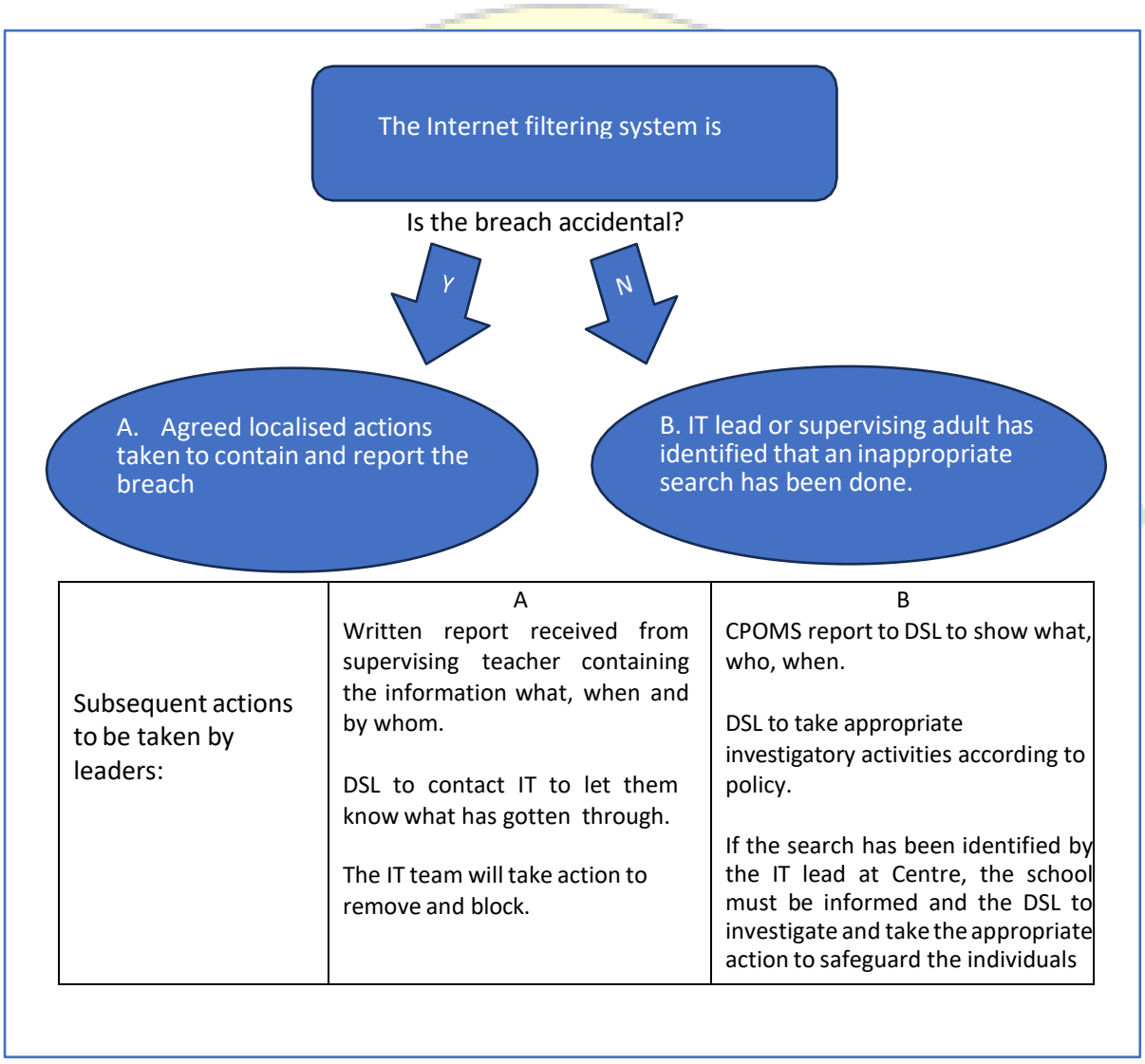
Schools will have a consistent, rapid localised response to the strategy they adopt when firewalls and filters are breached by inappropriate content. All staff and pupils must be aware of this process and can verbalise it clearly as well as use it.

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.



	A	B
Subsequent actions to be taken by leaders:	Written report received from supervising teacher containing the information what, when and by whom. DSL to contact IT to let them know what has gotten through. The IT team will take action to remove and block.	CPOMS report to DSL to show what, who, when. DSL to take appropriate investigatory activities according 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