

includEd Learning

Independent Specialist Education Provider



ONLINE SAFETY POLICY

Essential Safeguarding Information

KEEPING CHILDREN SAFE IN EDUCATION

We will adhere to the advice regarding all aspects of online safety including filtering and monitoring standards.

See KCSiE [Keeping Children Safe in Education 2025](#)

This online safety policy is linked to our:

- ☐ Child protection and safeguarding policy
- ☐ Behaviour policy
- ☐ Staff disciplinary procedures
- ☐ Data protection policy and privacy notices
- ☐ Complaints procedure

Author	N. Khan
Date agreed by Advisory Panel Body	October 2025
Review Date	October 2026
Signature	

Contents

Statement of Intent

1. Legal Framework	4
2. Roles & Responsibilities.....	5
3. Managing Online Safety	7
4. Cyber Bullying.....	8
5. Child-on Child Sexual Abuse and Harassment.....	9
6. Grooming and Exploitation	10
7. Mental Health.....	11
8. Online Hoaxes and Harmful Online Challenges.....	11
9. Cyber Crime.....	12
10. Online Safety Training for Staff.....	12
11. Online Safety and the Curriculum.....	13
12. Use of Technology in the Classroom.....	14
13. Use of Smart Technology	14
14. Educating Parents.....	15
15. Internet Access	16
16. Filtering and monitoring online activity	16
17. Network Security.....	17
18. Emails.....	17
19. Generative Artificial Intelligence (AI).....	17
20. Social Networking	18
21. The school website	19
22. Use of Devices	19
23. Remote learning	20
24. Monitoring and Review	20
Appendix 1 – Technology Acceptable Use	21
Appendix 2 – Acceptable Internet Use Pupils	23
Appendix 3 – Acceptable Internet Use Staff	24
Appendix 4 – Communications.....	26
Appendix 5 – Unsuitable/Inappropriate Activities	27
Appendix 6 – Incidents - Pupils.....	29
Appendix 7 – Incidents - Staff	30
Appendix 8 – Online safety Training - Self audit.....	31
Appendix 9 – Online Safety Incident Report Log	32

→ Statement of Intent

At IncludEd Learning, we are committed to the high quality use of ICT to enhance and enrich our curriculum. Our school aims to IncludEd Learning understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are several controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. This policy has been created with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils, staff and visitors.

→ 1. Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2026) 'Filtering and monitoring standards for schools and colleges'
- DfE (2026) 'Relationships and sex education (RSE) and health education'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2026) 'Keeping children safe in education 2026' (KCSIE)
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2025) 'Generative artificial intelligence in education'

- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people (updated March 2024)'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition' • National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

→ 2. Roles and Responsibilities

The advisory panel is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up to date by undertaking training.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges' filtering and monitoring standards.

The head of school is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up to date with current online safety issues and how the school is keeping pupils safe.
- Communicate regularly with parents to reinforce the importance of children being safe online.

- As part of the shortlisting process, consider carrying out an online search as part of their due diligence on shortlisted candidates to help identify any incidents or issues that have happened, and are publicly available online which the school/ academy might want to explore with applicants at interview.
- Working with the DSL and advisory panel to update this policy on an annual basis.

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT support staff.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the advisory panel about online safety on a termly basis.
- Working with the head and ICT support staff to conduct half-termly light-touch reviews of this policy.
- Working with the head and advisory panel to update this policy on an annual basis.

ICT support staff are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the head.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.

- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

→ 3. Managing Online Safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL/Head has overall responsibility for the school's approach to online safety, with support from deputies and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Sessions are conducted regularly on the topic of remaining safe online

Handling Online Safety Concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that pupils may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully and appropriate support provided to the victim.

Concerns regarding a staff member's online behaviour are reported to the head, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the head, it is reported to the LADO on 0161 234 1214..

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the head and ICT support staff, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behavioural Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the head will contact the police.

The school will avoid unnecessarily criminalising pupils. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL.

→ 4. Cyber Bullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating, discriminatory or upsetting messages
- Threatening or embarrassing media sent via electronic means
- Silent or abusive phone calls or using the victim's device to harass others, to make them think the victim is responsible
- Unpleasant or defamatory information/comments/messages posted online

- Abuse between young people in intimate relationships online

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

→ 5. Child-on-Child Sexual Abuse and Harassment

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Voyeurism and Upskirting
- Sexualised online bullying
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking “sides”, often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy. The school responds to all concerns regarding online child-on-child sexual abuse and harassment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with their child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

→ 6. Grooming and Exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including but not limited to:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay.

→ 7. Mental Health

The internet, particularly social media, can be the root cause of a number of mental health <https://portal.irisadapt.com/desktop.htmlh> issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media platforms and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

→ 8. Online Hoaxes and Harmful Online Challenges

For the purposes of this policy, an **“online hoax”** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **“harmful online challenges”** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils.

The DSL and head will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

→ 9. Cyber Crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL/head will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

→ 10. Online Safety Training for Staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours.

Staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

→ 11. Online Safety and the Curriculum

The school references the DfE 'teaching online safety in schools' guidance during the creation of their curriculum. Online safety is embedded throughout the curriculum and teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to use technology safely, respectfully and responsibly, including age-appropriate cyber security skills
- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online content, contact and conduct, and how to report concerns
- How to identify online risks, including how to protect their online identity and privacy •
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy and RSHE guidance

The online risks pupils may face online are always considered when developing the curriculum. The school's approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct and commerce.

The DSL is involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

→ 12. Use of Technology in the Classroom

A wide range of technology is used during lessons, including the following:

- Laptop/Desktop Computers
- Mobile/Tablet Devices
- Internet and Email
- Photo/Video/Audio equipment

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always review and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using technology and/or online materials during lesson time – this supervision is suitable to their age and ability.

→ 13. Use of Smart Technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of technology.

Pupils will not be permitted to use smart devices or any other personal technology during the school day without explicit permission and appropriate technological safeguards in place.

Where it is deemed necessary, the school will ban pupil's use of personal technology whilst on school site.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour Policy.

The school will hold sessions, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4C's (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

→ 12. Educating Parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.

Exposure to harmful content, e.g. content that encourages self-destructive behaviour. Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online is raised by the school via methods such as

- Letters and newsletters
- School website and links to external online resources, e.g. Child Exploitation and Online Protection Command (CEOP)
- High profile events, such as Safer Internet Day
- Online Reporting

→ 15. Internet Access

Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and agreed to an Acceptable Use Agreement.

All members of the school community are encouraged to use the school's network, instead of mobile networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately for their age group.

→ 16. Filtering and Monitoring Online Safety

The advisory panel will ensure the school has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The advisory panel will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding. The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

Requests regarding making changes to the filtering system will be directed to the Head and ICT support team.. Prior to making any changes to the filtering system, ICT technicians and senior leaders will review the request. Any changes made to the system will be recorded by ICT support staff. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT support staff, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Communication and Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure. If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

All staff will receive regular training on the operation and purpose of filtering and monitoring systems, including their role in safeguarding.

Personal devices connected to the school's network will be subject to the same filtering and monitoring standards to ensure consistent safeguarding measures.

Filtering and monitoring systems will undergo at least an annual review to assess their effectiveness and relevance.

→ 17. Network Security

A layered approach to security is taken at the school and is managed by ICT support staff. Antivirus security software is installed and kept up to date. Device firewalls are switched on at all times and application controls are employed to restrict access.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments and will be expected to report all malware and virus attacks to ICT support staff.

All members of staff have their own unique usernames and private passwords to access the school's systems. Pupils are provided with either their own unique username and private passwords or a shared account as appropriate. Staff members and pupils are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Users inform ICT support staff if they forget their login details, who will arrange for the user to access the systems under different login details. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time.

Users are required to lock access to devices and systems when they are not in use.

→ 18. Emails

Staff and pupils are given approved school email accounts. Prior to being authorised to use the email system, staff and pupils must agree to the Acceptable Use Agreement. Personal email accounts are not permitted to be used for school. Any email that contains sensitive or personal information is only sent securely via encrypted email.

Staff are not permitted to communicate with pupils or parents via personal email accounts.

Staff members and pupils are required report junk/phishing messages. The school's email system can is configured to reduce threats from emails and attachment.

Multi-Factor Authentication is enforced for all staff accounts and staff receive regular cyber security awareness training.

Any cyber-incidents are managed in line with the Data and Cyber-security Breach Prevention and Management Plan.

→ 19. Generative Artificial Intelligence (AI)

When deciding whether to use generative AI, safety will be the top priority. Any use of AI tools by staff and pupils will be carefully considered and assessed, evaluating the benefits and risks of its use in the school.

AI tools will only be used in situations where there are specified clear benefits that outweigh the risks, e.g. where it can reduce teacher workload, and the school will ensure that any use

of AI tools comply with wider statutory obligations, including those outlined in KCSIE.

Pupils will only be permitted to use generative AI in the school with appropriate safeguards in place, e.g. close supervision and the use of tools with appropriate filtering and monitoring features in place.

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

For any use of AI, the school will:

- Comply with age restrictions set by AI tools and open access large language models (LLMs).
- Consider online safety, including AI, when creating and implementing the school's approach to safeguarding and related policies and procedures.
- Consult KCSIE to ensure all statutory safeguarding obligations and AI tools are used safely and appropriately.
- Refer to the DfE's generative AI product safety expectations and filtering and monitoring standards.

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

→ 20. Social Networking

Personal use

Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson time. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Staff are not permitted to communicate with pupils or parents over social networking sites in an official capacity and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy.

Use on behalf of the school

The school's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the head to access the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

→ 21. The School Website

The head is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website.

→ 22. Use of Devices

School-owned devices

Staff members may be issued with devices such as laptops, tablets, mobile phones etc to assist with their work.

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum.

School-owned devices are used in accordance with the acceptable use agreements. Mobile school-owned devices are managed via a Mobile Device Management (MDM) Solution and are both encrypted and password protected.

ICT support staff monitor school-owned devices and automate the installation of software updates and antivirus definitions. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT support staff.

Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behavioural Policy respectively.

Personal devices

Any personal electronic device that is brought into school is the responsibility of the owner/user.

Students are not permitted to use personal devices on site during school hours without explicit permission of the school.

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members are not permitted to use their personal devices to take photos or videos of pupils. Staff members are not permitted to store student/staff personal data on personal devices.

Staff members must report concerns about their colleagues' use of personal devices on the school premises in line with the Allegations of Abuse Against Staff Policy.

Where a pupil uses accessibility features on a personal device to help them access education, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

→ 23. Remote Learning

All remote learning will be delivered in line with the school's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

→ 24. Monitoring and Review

The advisory panel, head/DSL review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is September 2027

Any changes made to this policy are communicated to all members of the school community.

→ Appendix 1: Technology Acceptable Use

IncludEd Learning 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.

User Accounts

- Pupil accounts are to be used by the assigned user / group for academy related and educational purposes, personal professional development and careers purposes only.
- Accessing or attempting to access another user's account is strictly prohibited.
- Pupils are required to take all necessary precautions to keep their account secure and must not share their personal account or password with others.

Use of Technology

- Pupils will only use systems and devices that they have been given permission to access.
- Pupils must adhere to the online safety guidelines they have been taught.
- Pupils must not store or use personal data relating to a pupil or staff member for non-school related activities on Trust systems and devices.
- At school, during school hours pupils must only use the internet for school related activities.
- Pupils must not attempt to download and run or install additional software on school owned devices.
- Pupils must delete emails from unknown senders without opening them and must not open any email attachments or links they contain.
- Pupils must behave responsibly and not interfere with teaching and learning whilst using systems and devices.
- Systems and devices are subject to UK law. Pupils must not use the systems to upload, download, use, retain, distribute, create or access any electronic materials which:
 - o May constitute a threat, bullying or harassment
 - o May be slanderous, abusive, indecent, obscene, racist, illegal or offensive.
 - o May be a breach of copyright and/or licence provisions
 - o Might gain access to restricted or unauthorised areas of the system and/or network, website or other hacking activities
- Pupils must not use the Trust systems for mass unsolicited mailings, commercial activity or the dissemination of junk mail, viruses or malware.
- Pupils must not attempt to "hack" or gain access to permissions, resources or systems that they are not permitted to access.

Personal Devices

- Direct connection to networks of devices not supplied by the school are not permitted.
- Pupils with permission to use a personal device, such as a laptop must connect to the guest Wi-Fi network at the school. Please speak to a member of ICT support for assistance.
- Personal mobile devices are prohibited during the school day and items such as mobile phones, tablets and media players must not be used on the school site and pupils must adhere to the school's mobile phone rules.
- Personal devices must not be used to record images/audio of other students or staff.

Social Media

- Pupils will not use devices to access personal social networking platforms
- Pupils must not communicate or attempt to communicate with staff members over personal social networking platforms or email.
- Pupils must not accept or send 'friend' or 'follow' requests from or to any staff member over personal social networking platforms
- Pupils must not publish any comments or posts about the school on any social networking platforms or websites which may affect the school's reputation.
- Pupils must 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 or platform.

Reporting Misuse

Pupils will ensure that they report misuse or breaches of this agreement by pupils or staff members by means of the school's reporting procedure

- Violations will be dealt with in line with the relevant policy e.g. Behavioural Policy or Child Protection and Safeguarding Policy

Agreement

I understand that my use of systems and devices including the internet will be monitored. I acknowledge that I have read and understood these terms and ensure that I will abide by each principle.

→ Appendix 2: Acceptable Internet Use - Pupils

This document is a guide to pupils to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I will only access the school network through my authorised username and password.
- I will not use the passwords of others.
- I will not use the school IT systems for personal or recreational use, for on-line gaming, gambling, internet shopping, file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any school computer or alter computer settings.
- I will hand in personal use my personal hand held devices (e.g. mobile phone/ipad) in school at times that are permitted. This is commuting to and from school, or to contact parents after participation in an extra- curricular activity. When using my own devices I understand that I have to follow the rules set out in this document.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them. For my own safety and that of others, I will not disclose personal information about myself or others when on-line.
- I will not arrange to meet 'on-line friends' unless I take an adult.
- I will not take, or distribute, images of anyone without their permission.
- I will only use chat and social networking sites with permission and at the times that are allowed.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line. Where the material I research on the Internet is protected by copyright,
- I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.

StudentName:	
Signed Student:	
Signed Parent/Carer:	Date:

→ Appendix 3: Acceptable Internet Use Staff

Responsible Use Agreement

I understand that I must use ICT systems in a responsible way ensuring no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the use of ICT for enhancing learning and will ensure all learners receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with students.

For my professional and personal safety:

- I understand that the school will monitor my use of ICT systems, email and other digital communications.
- I understand the rules set out in this agreement also apply to the use of the school ICT systems (e.g. laptops, email, website) out of the school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username and password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material/incident I become aware of to the appropriate person (see policy charts).

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images.
- I will not use my personal equipment to record these images. I will not use chat and social networking sites in the school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

IncludEd Learning, partner schools and the Local Authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (Ipads/laptops/mobile phones/USB devices etc) in the school, I will follow the rules set out in this agreement, in the same way as if I was using the school's equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems. I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not (unless I have permission) make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Sharing Information Policy. Where personal data is transferred outside the secure LA network, it must be encrypted.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by policy to disclose such information.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the Internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of ICT equipment in school, but also applies to my use of school ICT systems and equipment out of the school and my use of personal equipment in the school or in situations related to my employment by IncludEd Learning.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, suspension, referral to the Advisory Panel or the Local Authority and, in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use IncludEd's Learning ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer/Advisory Board Member

Name:	
Signed:	
Date:	

→ Appendix 4: Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

Communication Technologies	STAFF & OTHER ADULTS				PUPILS & YOUNG PEOPLE			
	Permitted	Permitted at certain times	Permitted for named staff	Not Permitted	Permitted	Permitted at certain times	Allowed with staff permission	Not permitted
Mobile phones May be brought to school	✓				✓			
Mobile phones used in lessons				✓				✓
Use of mobile phones in social time	✓				✓			
Taking photographs on mobile devices				✓				✓
Use of Ipads and other educational mobile devices		✓					✓	
Use of school email for personal emails				✓				✓
Social use of chat rooms/facilities				✓				✓
Use of social network sites			✓				✓	
Use of educational blogs	✓				✓			

→ Appendix 5: Unsuitable/Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyberbullying would be banned and could lead to criminal prosecution.

There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.

The school policy restricts certain internet usage as follows. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

Please see table below:

Acceptable/Unacceptable Activities

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					✓
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
Adult material that potentially breaches the Obscene Publications Act in the UK					✓
Criminally racist material in the UK					✓
Pornography					✓
Promotion of any kind of discrimination				✓	
Promotion of racial or religious hatred					✓
Threatening behaviour, including promotion of physical violence or mental harm					✓
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business				✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✓	
On-line gaming (educational)		✓			
On-line gaming (non-educational)				✓	
On-line gaming				✓	

→ Appendix 6: Incidents - Pupils

Incidents Involving pupils	Teacher to use school behaviour policy to deal with	Refer to pupil Head	Refer to police	Refer to technical support staff for action re security/filtering etc
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/		✓	✓	✓
On-line shopping / commerce	✓	✓		✓
File sharing	✓	✓		✓
Use of social networking sites	✓	✓		✓
Uploading to video broadcast e.g. Youtube	✓	✓		✓
Unauthorised use of non-educational sites during lessons	✓			✓
Unauthorised use of mobile phone/ digital camera/ other handheld device	✓			✓
Unauthorised use of social networking/ instant messaging/ personal email	✓	✓		✓
Unauthorised downloading or uploading of files		✓		✓
Allowing others to access school network by sharing username and passwords	✓	✓	✓	✓
Attempting to access or accessing the school network, using another student's account		✓		✓
Attempting to access or accessing the school network, using the account of a member of staff		✓		✓
Corrupting or destroying the data of other users		✓		✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓		✓
Continued infringements of the above, following previous warnings or sanctions		✓	Community Police Officer referral	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓		✓

→ Appendix 7: Incidents - Staff

Incidents involving members of staff	Refer to the Principal In event of breaches of policy by the Principal, refer to MSPRU	Refer to technical support staff for action re filtering, security etc	Referral to LADO Potential Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities)	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓	✓
Excessive or inappropriate personal use of the internet/social networking sites/ instant messaging/ personal email	✓	✓	✓
Unauthorised downloading or uploading of files	✓	✓	✓
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓	✓	✓
Careless use of personal data e.g. holding or transferring data in an insecure manner Deliberate actions to breach data protection or network security rules	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓
Using personal email/ social networking/ instant messaging/ text messaging to carrying out digital communications with students/ pupils	✓	✓	✓
Actions which could compromise the staff member's professional standing	✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓

→ Appendix 8: Online Safety Training Needs Self-Audit for Staff

Online Safety Training Needs Audit - Staff Self-Audit		
Name of staff member/volunteer:	Date:	
Question	Yes/No (add comments if necessary)	
Do you know the name of the person who has lead responsibility for online safety in school?		
Are you aware of the ways pupils can abuse their peers online?		
Do you know what you must do if a pupil approaches you with a concern or issue?		
Are you familiar with the school's acceptable use agreement for staff, volunteers, Advisory Panelnors and visitors?		
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?		
Are you familiar with the filtering and monitoring systems on the school's devices and networks?		
Do you understand your role and responsibilities in relation to filtering and monitoring?		
Do you regularly change your password for accessing the school's ICT systems?		
Are you familiar with the school's approach to tackling cyber-bullying?		
Are there any areas of online safety in which you would like training/further training?		

→ Appendix 9: Online Safety Incident Report Log

ONLINE SAFETY INCIDENT LOG

Online Safety Incident Report Log				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident