

Online Safety Guidance

Academic Year 2024-2027



In today's digital world, the internet is fundamental for education, business, and staying connected. Schools have a responsibility to equip learners with the skills to navigate this online environment safely and effectively. This means providing high-speed, reliable internet access that fosters a rich learning experience while prioritising online safety and responsible digital citizenship.

Through the use of the Internet and mobile devices, we ensure that the school equalities policy, safeguarding and curriculum prevent all forms of extremism and radicalisation.

Rationale

Online Safety reflects the need to raise awareness of the safety issues associated with information systems and electronic communication.

It encompasses not only internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the benefits of these technologies in educating children and young people, but also the risks and responsibilities of using them. It provides safeguards and raises awareness to enable users to control their online experiences.

Aims

This guidance identifies the measures in place in our Trust:

The 4 key Categories of risk

- **Content** –to protect pupils from undesirable content on the internet
- **Contact**- to protect pupils from undesirable contacts over the internet
- **Conduct**-to prevent unacceptable behaviour use of the internet by children or adults
- **Commerce**- to address issues of copyright, risks such as online gambling, inappropriate advertising, phishing and/or financial scams for materials published on the internet

Roles and Responsibilities

Online Safety is a whole-school responsibility dependent on all stakeholders, e.g., staff, parents, Trust Board, Local Governing Bodies. It is also up to the pupils themselves to ensure they act responsibly when using the internet and other forms of communication. The major consideration in creating a safe e-learning environment is internet-safety education, which occurs in the classroom itself and is initiated by the teacher or teaching assistant. Whilst the Headteacher has overall responsibility for online safety issues, and designated safeguarding lead's responsibility to manage online safety issues and incidents in line with the school child protection policy.

Governors will ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the

importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

Education

The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:

- Ensuring education regarding safe and responsible use precedes internet access
- Reinforcing online safety messages whenever technology or the internet is in use
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval, and evaluation
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Permission to Use the Internet

The Internet can provide pupils and all stakeholders with opportunities to experience and access a wide range of activities, resources, and information to support and enhance learning and teaching across the whole school curriculum. All pupils will be expected to access the internet unless parents indicate otherwise at the time their child is admitted to school.

Online Safety documents will be published on the website for everyone to access.

Accessing and Using the Internet

Pupils use individual logins whenever possible. Pupils will be taught to use the internet safely and responsibly as an integral part of e-learning across the curriculum, supported by the school's Online Safety policy. Pupils will be taught how to keep themselves safe whilst online at home as well as at school.

Content

Unintentional Exposure of Children to Inappropriate Content

It is the intention of the Connect Education Trust that all reasonable steps will be taken to prevent exposure to pupils of undesirable materials and inappropriate content on the internet. However, it is recognised that this can happen not only through deliberate searching for such materials but also unintentionally when a justifiable internet search produces unexpected results.

To protect pupils from such occurrences, the school has adopted the following position:

- Adult supervision of pupils' internet activity, with access or searching on the internet **only allowed** with a suitable adult present in the room
- The "caching" of internet sites by staff, whenever possible in advance, to verify the site and its content
- Pupils being taught to become critical and discriminating users of materials they find online, through questioning the source and reliability of any content they access, and by being aware of ways to minimise risks.

Intentional Access to Undesirable Content by Pupils

Pupils should never intentionally seek offensive material on the internet. Any such incident will be treated as a disciplinary matter, and the parents will be informed.

In the event of pupils gaining access to undesirable materials, the following steps will be taken:

- The teacher will report the incident to the DSL/ Headteacher
- The incident will be recorded in a central log located in the school, and a Serious Incident Form completed. The school will reliably report the frequency and nature of incidents to any appropriate party
- Parents will be notified at the discretion of the Headteacher and according to the degree of seriousness of the incident. For example, exposure to materials that include common profanities might not be reported to parents, but exposure to materials that include pornographic images would be reported
- The Headteacher will regularly notify the Trust Board, Local Governing Bodies. of any incidents involving inappropriate or unacceptable use of school internet/ICT facilities as part of the Headteacher's report/ update

Intentional Access to Undesirable Content by Adults

Deliberate access to undesirable materials by adults is unacceptable and will be treated as a disciplinary issue. If abuse is found to be repeated, flagrant or habitual, the matter will be treated as a very serious disciplinary issue.

Risks Associated with Contact

The internet as a means to contact people and organisations is an extremely valuable tool, encouraging the development of communication skills and transforming the learning process by opening up extra possibilities. However, just as in the real world, pupils may become involved in inappropriate antisocial or illegal behaviour whilst using new technologies e.g., cyber bullying, identity theft or arranging to meet people they have met online.

Whilst pupils will at times use email as part of their learning across the curriculum, the school does not use chat rooms or instant messaging. Pupils will be made aware of the risks involved in all of these and ways of avoiding them as part of their learning.

Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules
- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
 - Delete the material, or
 - Retain it as evidence (of a possible criminal offence* or a breach of school discipline), and/or
 - Report it to the police**

* If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#).

** Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

Any searching of pupils will be carried out in line with:

The DfE's guidance on [searching, screening and confiscation](#)

UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Receiving and Sending of Emails by Pupils

It is recognised that email messages received by pupils can contain language or content that is unacceptable and that some people may try to use email to identify and contact pupils for unacceptable reasons. If any member of staff believes that a pupil has been targeted with email messages by parties with criminal intent, the messages will be retained. The incident will be recorded, and the child's parents will be informed. Advice will also be taken regarding possible further steps.

To avoid these potential issues the Trust has adopted the following practices:

- The use of the accredited email service which includes the filtering of all incoming and outgoing messages for inappropriate content and spam
- Pupils only read email messages when a member of staff is present, or the messages have been previewed by the member of staff
- Pupils are taught not to open or respond to emails from a previously unknown source, but to tell the member of staff present in the room so that appropriate action can be taken
- Steps are taken to verify the identity of any school or person seeking to establish regular email contact with this school
- Pupils save their emails messages to 'draft' for the member of staff to approve before being sent
- To prevent pupils revealing their identity within email messages, only the pupil's forename is revealed, and this is only when appropriate.

Publishing Pupil's Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the school website or learning platform particularly in association with photographs. This includes in file names or in the <ALT> tag. Full names will not be published in any media produced by the school.
- Written permission from parents will be obtained before photographs of pupils are published on the internet. No pupils who the Designated safeguarding Lead feel are at particular risk will have their images shown.
- Pupil's work can only be published with the permission of the pupil and parents (age related)
- If parents wish to take photos/video of school events e. g assemblies, concerts these must be for your own private/personal use and must not be used inappropriately
- Please do not obscure the view of others when taking photos

The Use of Social Networking and Online Media

The Connect Education Trust asks its whole community to promote the three common approaches to online behaviour:

- Common courtesy
- Common decency
- Common sense

How Do We Show Common Courtesy Online?

- We ask someone's permission before uploading photographs, videos or any other information about them online
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials because to do so is disrespectful and may upset, distress, bully or harass

How Do We Show Common Decency Online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is online bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How Do We Show Common Sense Online?

- We think before we click
- We think before we upload comments, photographs and videos
- We think before we download or forward any materials
- We think carefully about what information we share with others online
- We check where it is saved and check our privacy settings
- We make sure we understand changes in use of any websites we use
- We block harassing communications and report any abuse

Any actions online that impact on the Trust or school (or someone in the school) and can potentially lower the reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, pupil or parent is found to be posting libellous or inflammatory comments any social network sites, they will be reported to the appropriate 'report abuse' section of the network site.

All social network sites have clear rules about the content which can be posted on the site, and they provide robust mechanisms to report content or activity which breaches this.

Any breach of serious cases this may lead to disciplinary action under the Trust disciplinary policy/code of conduct. Serious breaches, such as incidents of bullying or of social media activity causing damage to the organisation, may constitute gross misconduct and could lead to dismissal.

Use of Social Networking by Staff in a Personal Capacity

The Trust is aware and acknowledges that increasing numbers of adults and pupils are using social networking sites. Some with the widest use are Instagram, Facebook and Twitter. The widespread availability and use of social networking application bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our reputation.

The purpose of this guidance is to ensure:

- That the Trust is not exposed to legal risks
- That the reputation of the Trust is not adversely affected

- That our users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the Trust.

This guidance covers the use of social networking applications by all Trust/ school stakeholders, including employees, pupils, and those in voluntary and governance roles. These groups are referred to collectively as 'school representatives' for brevity.

The requirements of this guidance apply to all uses of social networking applications which are used for any Trust related purpose and regardless of whether the Trust representatives are contributing in an official capacity to social networking applications provided by external organisations.

Social networking applications include, but are not limited to: Blogs, for example Blogger Online discussion forums, such as Netmums.com, Collaborative spaces such as Facebook, media sharing services, for example YouTube and 'Micro-blogging' applications, for example Twitter.

All school representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.

They must also operate in line with the Trust's equality policy and code of conduct. Use of social networking sites or the use of social networking applications in work time for personal use only is not permitted, unless permission has been given by the Headteacher.

Social Networking as part of a school service (whether they are hosted by the school or by a third party) must be approved by the Headteacher/ CEO first.

Guidelines For Staff

- Staff must **never** add pupils as 'friends' into their personal accounts (including past pupils under the age of 16)
- Staff are **strongly advised** not to add parents as 'friends' into their personal accounts
- Staff **must not** post comments about the Trust/ school, pupils, parents or colleagues, including members of the Trust Board or Local Education Committee
- Staff must not use social networking sites within working hours (for personal use)
- Staff should only use social networking in a way that does not conflict with the current National Teacher's Standards

- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality
- Staff should read and comply with the guidance for Safer Working Practice for Adults who Work with Children and Young People
- Inappropriate use by staff should be referred to the Headteacher/ CEO in the first instance and may lead to disciplinary action

Other Use of the Internet and Email Facilities

The Trust internet/email facilities should be used only for educational purposes during teaching and learning time/ working hours. If a member of staff chooses to use school internet facilities for personal purposes, such as online banking or purchasing of items for personal use, they do so at their own risk. Staff who have their own children at a school within the Trust, or whose children have social contact with Connect Education Trust pupils must be extra vigilant when accessing social network sites.

Staff must be aware of and make sure they understand the dangers of using social networking sites. Staff using these sites must ensure they have high security settings and must not disclose Trust information.

Use of Email

Under Education law regarding data protection and record-keeping (such as the General Data Protection Regulation (GDPR) in the UK), staff should solely utilise their school email accounts for official school business. This ensures a clear separation between personal and professional communication and safeguards. The Trust has the right to reset staff passwords and access email content if necessary for educational purposes or investigations, promoting transparency and accountability within the school.

Communication with Pupils Through Technology

Adults or volunteers who work with pupils should be mindful of how they use social media and the potential for others to access personal content they may post. Staff should maintain a clear boundary between personal and professional communication and use a privacy setting on personal accounts so that these are not accessible to pupils. Staff should:

- Have security settings to the maximum
- Do not allow any Connect Education Trust pupils or parents to see their profile
- Do not use their profile to bring the Trust/ school or an individual into disrepute (including all stakeholders)

- Staff must not use their personal mobile or personal device during working hours e.g. photography on personal mobile
- Disciplinary action may result if these boundaries are not adhered to

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation & Cyber security.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

Education and Engagement With Pupils

The school curriculum includes age-appropriate lessons and activities on online safety for all pupils, intended to raise awareness, build resilience, and promote safe and responsible internet use by:

- Ensuring education regarding safe and responsible use precedes internet access
- Including online safety across the curriculum, including Personal Social and Health Education, Relationships and Sex Education and Computing programmes of study, covering use both at school and home
- Reinforcing online safety messages whenever technology or the internet is in use
- Ensuring that the needs of pupils considered to be more vulnerable online, such as those with SEND or mental health needs, are met appropriately
- Using support, such as peer education approaches and external visitors, to complement online safety education in the curriculum
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Teaching pupils to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Supporting students 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

Awareness and Engagement With Parents

Parents have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies. The school will build a partnership approach to online safety with parents by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events
- Drawing parents' attention to the school's online safety policy and expectations in newsletters and on the website
- Requiring parents to read the pupil's Acceptable Use Agreement and discuss its implications with their children.

Managing Personal Data Online

Personal data will be recorded, processed, transferred, and made available online in accordance with the General Data Protection Regulations (GDPR) and Data Protection legislation.

Further GDPR Guidance & Information can be found in the following policies:

- Data Protection Policy
- Code of Conduct
- Privacy Notices
- Management of Records and Guidance Information
- Child protection and Safety Guarding
- Behaviour Policy
- Complaints Procedures
- Cyber security guidance

Online Radicalisation and Extremism

The Trust will take all reasonable precautions to ensure that pupils are safe from terrorist and extremist material when accessing the internet in school

If the school is concerned that a pupil or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately, and action will be taken in line with the Safeguarding and Child Protection policy.

If the school is concerned that members of staff may be at risk of radicalisation online, the Headteacher and the Trust will be informed immediately, and action will be taken in line with the Safeguarding and Child Protection policy.

Remote Education - The DfE's [Providing remote education: guidance for schools](#) after the expiration of the temporary provisions in the Coronavirus Act 2020 in relation to remote education.

Staff Working Remotely

Working remotely and accessing personal data from outside of the Trust presents risks we need to be aware of to keep staff, pupils and their data safe.

- Staff members must use secure passwords and keep these safe. They must not be accessible by others.
- Devices must always be locked when not in use.

- Staff should always have access to their 2-factor key
- Staff must only use official communication when communicating personal information about staff and pupils such as the Trust emails and drives
- Staff using Trust devices for work should always use them for accessing Trust data and websites. This device should have appropriate controls and safeguards in place to ensure that data is kept secure. Trust devices are for employees only and should not be used by any other members of the family or household.
- Staff should not use personal devices for work-related activity.
- Staff and pupils should always be aware of phishing emails and should pay particular attention to the following
 - senders email address that does not match the organisation’s address
 - spelling / grammatical mistakes
 - urgency in requests for action
- Staff and pupils should not save any personal data and instead use the approved tools and services already provided by the trust. Files and resources can be saved to Google Drive
- Staff and pupils must stay alert and report anything that they are unsure of. If something looks or seems not right, it probably is not.

Use of Mobile Phones

Schools have the authority to decide whether pupils can bring their mobile phones to school. If allowed, there should be a system for collecting and returning the phones at the end of the day, and schools are responsible for ensuring that acceptable usage for mobile phones is established and set expectations. [Click here for further guidance.](#)

Appropriate Filtering and Monitoring

The Connect Education Trust is committed to doing all we can to limit children’s exposure to online risks from the school’s IT system. Keeping Children Safe in Education obliges schools to “ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

The DSL will take lead responsibility for safeguarding and child protection across the school (including online safety and understanding the filtering and monitoring systems and processes in place)

This Cybersecurity guidelines and security provisions which are there to protect our systems, services and data in the event of a cyberattack. **(Please see Cybersecurity Incident Response Plan guidance)**

Cloud Platform

It is important to consider data protection before adopting a cloud platform or service – see our Data Protection Policy. The Connect Education Trust adheres to the principles of the Department for Education document [Cloud computing services: guidance for school leaders, school staff and Governing Bodies](#).

The Trust has adopted GSuite so most data should be stored on GSuite to ensure data security unless there is a 3rd party tool in place.

The following principles apply:

- The DPO approves new cloud systems, what may or may not be stored in them and by whom.
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such.
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication keys is used by staff for access to highly sensitive documents
- Only school-approved platforms are used by pupils or staff to store pupil work.

Copyright

It is recognised that all materials on the internet are subject to copyright unless the copyright is specifically waived. It is the Trust's policy that the copyright of internet materials will be respected.

Where materials are published on the internet as part of the teacher's professional duties, copyright will remain with the Trust. Internet published materials will contain due copyright acknowledgements for any third-party materials included within them.

Incident Reporting

You should report any actual security breaches or attempted security breaches, to the Data Protection Officer immediately – connectdpo@excathedra.solutions

Concerns regarding viruses, phishing emails, unsolicited emails, any unauthorised use or suspected misuse of ICT or any matter of concern, should be reported to your manager and to relevant ICT staff as a matter of urgency.

This policy should be read in conjunction with the Trust's Safeguarding and Child Protection Policy, AI guidance, Cyber Security, IT Acceptable Use policy and the social media guidance.

Useful Links and Resources

- [Teaching Online Safety in School \(DfE\)](#)
- [Education for a Connected World \(UKCIS\)](#)
- [Sharing nudes and semi-nudes: advice for education settings working with children and young people \(UKCIS\)](#)
- [Indecent images of children: guidance for young people](#)
- [Cyberbullying: understand, prevent and respond \(Childnet\)](#)
- [Cyberbullying: advice for headteachers and school staff \(DfE\)](#)
- [Cyberbullying-\[www.cyberbullying.org\]\(http://www.cyberbullying.org\)](http://www.cyberbullying.org)
- [Cybersecurity standards](#)
- [GDPR- <https://ico.org.uk/for-organisations/guide-to-data-protection>](https://ico.org.uk/for-organisations/guide-to-data-protection)
- [NCSC Cyber Security Training](#)
- CEOP: www.thinkuknow.co.uk
- www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- NSPCC: www.nspcc.org.uk/onlinesafety o ChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- [Education for a Connected World](#)
- [Mobile phones in School](#)