Coláiste de hÍde

Meas – Bród – Comhar

Bóthar Chaisleán Thigh Motháin, Tamhlacht, Baile Átha Cliath 24.
Fón 01 4513984 **Facs** 01 4527075 **R-phost**: eolas@colaistedehide.ie
Suíomh Idirlín www.colaistedehide.ie

Internet Acceptable Use Policy

Content

General Approach and Coláiste de hÍde's Mission Statement

Tá sé mar aidhm againn i gColáiste de hÍde an bóthar a réiteach do gach aon dalta a lánacmhainn a bhaint amach le héascaíocht, go hintleachtúil, go fisiciúil, go spioradálta, go cultúrtha, go sóisialta agus go mothálach tré mheán na Gaeilge. Déantar iarracht ar leith ins an scoil féiníomhá dearfach a chothú i ngach aon duine, maille le meas a chothú iontu do gach duine, dá dtimpeallacht agus dá bpobal.

The aim of this Acceptable Use Policy is to ensure that students will benefit from learning opportunities offered by the school's digital resources in a safe and effective manner. The responsible use of internet and digital technologies, both online and offline and access is considered an integral part of teaching and learning. Therefore, if the school AUP is not adhered to agreed sanctions will be imposed.

When using the internet students, parents and staff are expected:

- To always treat others with respect.
- Not undertake any actions that may bring the school into disrepute.
- Respect the right to privacy of all other members of the school community.
- Respect copyright and acknowledge creators when using online content and resources.

The school employs several strategies to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

- Filtering software and/or equivalent systems will be used to minimise the risk of exposure to inappropriate material.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.

This Acceptable Use Policy applies to students who have access to and are users of the internet in Coláiste de hÍde. It also applies to members of staff, volunteers, parents, carers and others who access the internet in Coláiste de hÍde.

Misuse of the internet may result in disciplinary action, including withdrawal of access privileges, detention and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

Coláiste de hÍde may deal with incidents that take place outside the school that impact on the wellbeing of students or staff under this policy, the Code of Behaviour, our Bí Cineálta Policy and other associated policies. In such cases Coláiste de hÍde may, where known, inform parents/guardians of incidents of inappropriate online behaviour that take place out of school and impose the appropriate sanctions.

Coláiste de hÍde implements the following strategies on promoting safer use of the internet:

- Students will be provided with education around internet safety as part of our implementation of Wellbeing, SPHE and other curriculum areas.
- Teachers are encouraged to engage with continuing professional development opportunities in internet safety.

This policy and its implementation may be reviewed by the following stakeholders: Board of Management, Staff, Students and Parents.

Should serious online safety incidents take place, school management and the Gardaí should be informed.

Content Filtering

Coláiste de hÍde has chosen to implement the following level on content filtering on the Schools Broadband Network:

Split Level - This level allows different filtering levels for different ages / stages and different groups of users; staff / visitors / students etc.

Students taking steps to by-pass the content filter by using proxy sites or other means may be subject to disciplinary action, including withdrawal of access privileges, detention and, in extreme cases, suspension or expulsion.

Internet Use

- Students will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.

- Students will be encouraged to report accidental accessing of inappropriate materials in accordance with school procedures.

- Students will report accidental accessing of inappropriate materials in school but outside the classroom to their class tutor and/or year head.

- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).

- Students and staff will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

- Students will use the Internet for educational purposes only.

- Students will not engage in online activities such as uploading or downloading large files that result in heavy network traffic which impairs the service for other internet users.

- Students will not download or view any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.

- Downloading by students of materials or images not relevant to their studies is in direct breach of the school's acceptable use policy.

- Students will never disclose or publicise personal information or passwords.

- Students will be aware that any usage of the internet and school's digital platform, including distributing or receiving information, school-related or personal, will be monitored.

Email and Messaging

- The use of personal email accounts is not allowed at Coláiste de hÍde.
  - Students will use approved school email accounts.
  - Students should not under any circumstances share their email account login details with other students.
  - Students should not use school email accounts to register for online services such as social networking services, apps, and games.
  - Students should be aware that email communications are monitored.

- Students will not send any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.

- Downloading by students of materials or images not relevant to their studies is not allowed.

- Students should immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Students should avoid opening emails that appear suspicious. If in doubt, students should ask their teacher before opening emails from unknown senders.

- Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.

- Students will never arrange a face-to-face meeting with someone they only know through emails or the internet.

- Students will not forward email messages or screenshots of emails or "reply all" without the permission of the originator

- Students must only use their school email for school related activities and for registering on school-based activities only. The use of personal email addresses is not allowed for school-based work.

- Students should not use school email accounts to register for online services, social networking, apps or games.

- Students should report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Students should report any such communications to a teacher.

- All emails and opinions expressed in email are the responsibility of the author and do not reflect the opinion of the school.

Social Media and messaging services for Staff and Students

The internet provides a range of social media tools that allow us to interact and keep in touch. While recognising the benefits of these media for new opportunities for communication, this policy sets out the principles that members of our school community are expected to follow when using social media.

The principles set out in this policy are designed to help ensure that social media is used responsibly so that the confidentiality of students, staff and the reputation of the school is protected.

This policy applies to personal websites such as social networking sites (for example Instagram and TikTok), blogs, microblogs such as X, chatrooms, forums, podcasts, open access online encyclopaedias such as Wikipedia, social bookmarking sites such as del.icio.us and content sharing sites such as flickr and YouTube. The internet is a fast-moving technology, and it is impossible to cover all circumstances or emerging media.

The following statements apply to the use of messaging, blogging and video streaming services in Coláiste de hÍde:

- Use of instant messaging services and apps including Snapchat, WhatsApp, Viber, etc. is not allowed in Coláiste de hÍde.
- Use of blogs such as WordPress, Tumblr etc. is allowed in Coláiste de hÍde with express permission from teaching staff.
- Use of video streaming sites such as YouTube and Vimeo etc. is with express permission from teaching staff.

- All members of the school community must not use social media, messaging services and the internet in any way to harass, impersonate, insult, abuse or defame others.

- Staff and students must not discuss personal information about students, staff and other members of the Coláiste de hÍde community on social media.

- Staff and students must not use school email addresses for setting up personal social media accounts or to communicate through such media.

- Staff and students must not engage in activities involving social media which might bring Coláiste de hÍde into disrepute.

- Staff and Students must not represent your personal views as those of bring Coláiste de hÍde on any social medium.

- Students will be provided with guidance on etiquette regarding social media.

Teachers can read further information about the use of Social Media and Electronic Communication here:

https://www.teachingcouncil.ie/en/news-events/latest-news/2021/guidance-for-registered-teachers-about-the-use-of-social-media-and-electronic-communication.html

Personal Devices

The following statements apply to the use of internet-enabled devices such as tablets, gaming devices, smartwatches, in Coláiste de hÍde:

- Students are not allowed to bring personal internet-enabled devices into Coláiste de hÍde.

Digital Learning Platforms (including video conferencing)

Coláiste de hÍde digital learning platform is owned and managed by the school. The school currently uses Google and Microsoft as digital learning platforms, these platform should enable two-way communication between staff and students and amongst staff members.

- Students must only use their school email for accessing the school digital learning platform.
- Only school devices should be used for the purposes of capturing and storing media.
- All school-related media and data should be stored on the school's platform.
- Each user of the platform will be provided with their own unique login credentials.
- Passwords for digital platforms and accounts should not be shared.
- Personal email addresses should not be used when creating accounts on school digital platforms.

Audio, images and video

- Photo permissions for students can be easily granted or revoked by parents at any time via our school app, managed by Unique Schools.

- Care should be taken when capturing audio, photographic or video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- At Coláiste de hÍde students must not record audio, take, use, share, publish or distribute images of others without their permission.

- Recording audio, taking photos or videos on school grounds or when participating in school activities is only allowed with expressed permission from staff.

- Students must not share audio, images, videos or other content online with the intention to harm another member of the school community regardless of whether this happens in school or outside.

- Sharing explicit images/video and in particular explicit images/video of students and/or minors is an unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved. Sharing explicit images/video of other students automatically incurs suspension as a sanction.

Inappropriate Activities

- Misuse and fraud legislation
- Racist material
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Harmful content or 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 (e.g. 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
- Online gaming
- Online gambling
- Online shopping
- Use of social networking sites, instant messaging and online forums
- Child sexual abuse material
- Any other activity considered questionable

School Websites

Students will be given the opportunity to publish projects, artwork or schoolwork on the internet in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website.

Students will continue to own the copyright on any work published.

The website will be regularly checked to ensure that there is no content that compromises the safety, privacy, or reputation of students or staff.

Coláiste de hÍde will use only digital photographs, audio or video clips of focusing on group activities. Content focusing on individual students may be published with parental permission.

The publication of student work will be coordinated by a teacher.

Personal student information including home address and contact details will not be published on Coláiste de hÍde web pages.

Cyberbullying

In accordance with the Anti-Bullying Procedures for Schools, Coláiste de hÍde considers that posting a single harmful message/image/video online which is highly likely to be reposted or shared with others can however be seen as bullying behaviour.

This type of bullying is increasingly common and is continuously evolving. It is bullying carried out using information and communication technologies such as text, social media, e-mail, messaging, apps, gaming sites, chatrooms and other online technologies. Being the target of inappropriate or hurtful messages is the most common form of online bullying. As cyberbullying uses technology to perpetrate bullying behaviour and does not require face to face contact, cyberbullying can occur at any time (day or night). Many forms of bullying can be facilitated through cyberbullying.

Access to technology means that cyberbullying can happen around the clock and the students' home may not even be a safe haven from such bullying. Students are increasingly communicating in ways that are often unknown to adults and free from supervision. The nature of these technologies means digital content can be shared and seen by a very wide audience almost instantly and is almost impossible to delete permanently. While cyberbullying often takes place at home and at night, the impact can also be felt in school.

In accordance with our Bí Cineálta Policy, Coláiste de hÍde considers that a once-off offensive or hurtful public message, image or statement on a social network site or other public forum where that message, image or statement can be viewed and/or repeated by other people may be regarded as bullying behaviour.

When using the internet students, parents and staff are expected to always treat others with respect.

Engaging in online activities with the intention to harm, harass, or embarrass another student or member of staff is an unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved.

Measures are taken by Coláiste de hÍde to ensure that staff and students are aware that bullying is defined as targeted behaviour, online or offline, that causes harm. The harm caused can be physical, social and/or emotional in nature. Bullying behaviour is repeated over time and involves an imbalance of power in relationships between two people or groups of people in society. Posting a single harmful message/image/video online which is highly likely to be reposted or shared with others can however be seen as bullying behaviour.

The prevention of cyberbullying is an integral part of the anti-bullying policy of our school.

In accordance with the Department of Education Bí Cineálta Procedures to Prevent and Address Bullying Behaviour for Primary and Post Primary Schools; Coláiste de hÍde considers that a school is not expected to deal with bullying behaviour that occurs when students are not under the care or responsibility of the school. However, where this bullying behaviour has an impact in school, schools are required to support the students involved. Where the bullying behaviour continues in school, schools should deal with it in accordance with their Bí Cineálta Policy.

Artificial Intelligence

Coláiste de hÍde recognises the potential benefits of Artificial Intelligence (AI) in education and is committed to its responsible and ethical use within our learning environment.

- Coláiste de hÍde provides and promotes training and professional development opportunities for teachers to effectively utilise AI tools in their teaching practices, ensuring they stay up to date with technological advancements.

- All AI tools authorised for use in Coláiste de hÍde comply with data protection regulations (GDPR). Entering personal, sensitive, or confidential data into any AI system without proper authorisation is strictly prohibited.

- Coláiste de hÍde integrates AI into its educational processes to enhance learning, foster innovation, and promote the development of critical skills. AI technologies are integrated into the curriculum to enhance learner outcomes and experiences. The selection of AI tools and technologies in Coláiste de hÍde aligns with educational goals, including supporting learner agency and promoting critical thinking.

- Coláiste de hÍde will make necessary adjustments to our school's adoption and integration of AI, based on review and feedback, including our Assessment Policy.

- School staff and learners are encouraged to think of the ethical use of AI technologies, including understanding data privacy, identifying biases, and verifying AI-generated information.

- Learners will not create, share or send any AI generated material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person. Staff and learners must not engage in activities involving AI generated material which might bring Coláiste de hÍde into disrepute.

- Staff and learners must not use AI in any way to harass, insult, abuse or defame learners, their family members, staff, other members of the Coláiste de hÍde community.

- Coláiste de hÍde promotes digital literacy and critical thinking skills to help learners understand AI, its implications, and responsible usage. This includes data literacy, verification of AI-generated information, and recognising potential biases in AI tools.

- AI generated material is allowed for the purpose of research, brainstorming, revising text. Teachers will attribute AI text and images when used. Learners must attribute AI text and images properly when used in assignments/homework. If used for research learners must factcheck, check other sources and reference sources.

Legislation

The following legislation relates to use of the Internet which teachers, students and parents should familiarise themselves with:

- Data Protection Acts 1988 to 2018 and General Data Protection Regulations (GDPR)
- Copyright and Related Rights Act 2000
- Child Trafficking and Pornography Act 1998 and Criminal Law (Sexual Offences) Act 2017
- Children First Act 2015
- Harassment, Harmful Communications and Related Offences Act 2020 (Coco's Law)
- Criminal Damage Act 1991

Support Structures

The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

Sanctions

Misuse of the Internet and digital technologies should be referred to in the school's Code of Behaviour and Bí Cineálta Policy and related sanctions regarding misuse as appropriate should be outlined therein. The school also reserves the right to report any illegal activities to the appropriate authorities, including An Garda Síochána.

Response to recent developments in relation to AI-Generated nudification apps

In light of recent concerns highlighted in the media regarding the misuse of Artificial Intelligence (AI) technologies to create non-consensual images, the department, in collaboration with Webwise, published updated information and guidance for parents and schools on the risks, harms and safeguarding issues associated with AI-generated nudification apps on 9 January 2026. This resource is intended to support schools in engaging with parents and students on these issues and forms part of the department's wider online safety and digital citizenship supports.

This new guidance is available at:

- www.webwise.ie/news/nudification-apps-information-and-guidance-for-parents and-schools

Supporting schools and parents to protect children online

Webwise (the department and EU funded internet safety initiative) continues to develop and disseminate resources that help teachers integrate digital citizenship and online safety into teaching and learning in their schools. Webwise also provides information, advice, and tools to parents to support their engagement in their children's online lives via:

- www.webwise.ie

With the help of the Webwise Youth Advisory Panel, Webwise develops youth-oriented awareness raising resources and training programmes that promote digital citizenship and address topics such as online wellbeing, cyberbullying and more.

Online safety and the curriculum

Online safety is addressed through the curriculum at primary and post-primary level, with training and supports in place, for example, for teachers of Wellbeing and SPHE (Social, Personal and Health Education).

At primary school level, the recently launched redeveloped Wellbeing specification includes outcomes focused on Media and Digital Wellbeing, supporting safe and ethical use of technology and understanding media influence. The module "Learning about media and digital wellbeing" (Stages 1-4) equips children to navigate media and the digital world safely and responsibly, helping them to develop a balanced and informed relationship with media and technology.

At post-primary level, SPHE specifications have been redeveloped and updated and teaching and learning resources have been developed to support teachers. SPHE must be offered to all Junior Cycle students and, from September 2027 to all Senior Cycle students. These specifications aim to equip children and young people with the skills, dispositions, values and attitudes to lead fulfilling and healthy lives, to have respectful and loving relationships and to be able to navigate the world around them.

The Junior Cycle SPHE specification includes a number of learning outcomes that relate to social media and the online world, including for example that students should be able to assess the benefits and difficulties associated with their online world, as well as discussing how to share personal information, images, opinions and emotions in a safe, responsible and respectful manner online. Also at Senior Cycle, SPHE learning outcomes empower students with the skills needed for nurturing healthy relationships both in-person and online relationships, including respecting boundaries, communicating feelings and needs and preventing and managing conflict.

Senior Cycle SPHE students also examine how harmful attitudes around gender are perpetuated in the media, online and in society and learn about their rights and responsibilities before the law as a young adult with reference, among other contexts, to online communicating.

Teacher Professional Learning (TPL)

Oide, the department funded support service for teachers and school leaders, provides a variety of professional learning to teachers.

The Oide Wellbeing team support teachers and schools, through the SPHE curriculum, to develop and promote the personal development, health and wellbeing of the student, to create a positive school environment and culture, and to prevent and tackle bullying, including online bullying and harassment.

Schools are notified regularly with regard to Oide's wide-ranging offerings of professional learning events and school leaders/teachers can register for any event. TPL resources available to schools include a wide range of classroom resources and materials, including online self-directed courses, all of which can be accessed/downloaded by visiting the following:

- www.oide.ie

Oide Technology in Education (TiE) promotes and supports the integration of digital technologies in teaching, learning and assessment in primary and post-primary schools. Oide TIE offers a range of professional learning supports, including online courses, webinars, good practice videos, and digital learning resources. Additionally, professional learning is facilitated through the Education Support Centre Network (ESCI), and direct support for schools is available from the digital technology teams. • www.oidetechnologyineducation.ie

Acceptable Use Policy

All schools are required to have an Acceptable Use Policy (AUP) setting out rights, responsibilities, and sanctions for the use of the internet and digital technologies in their schools, including social media in line with the Webwise guidance "Acceptable Use Policy Guidelines: Guidelines for developing an Acceptable Use Policy in school"

These guidelines are available below by visiting:

- www.webwise.ie/teachers/acceptable-use-policy/how-to-develop-an acceptable-use-policy/

The primary purpose is to promote safe, responsible use and to address risks associated with online activity in the school.

AUPs are expected to explicitly address online communication, including email, social media, online forums and messaging services, alongside filtering, monitoring and reporting mechanisms.

Existing guidance does not promote routine use of public social media platforms in schools. Instead, it requires schools to set their own clear rules through their AUPs, apply filtering and supervision, restrict access to inappropriate services, and educate students in safe and responsible online behaviour, with strong child protection and reporting mechanisms in place.

Acceptable Use Policy - social media use

The AUP guidance states that staff and students must not use social media or messaging services to

harass, impersonate, insult, abuse or defame others, disclose personal information, bring the school into disrepute, or represent personal views as those of the school.

Students are provided with guidance on appropriate online etiquette, and schools may direct staff to Guidance for Registered Teachers by the Teaching Council about the use of social media and electronic communication.

This guidance is available below by visiting:

- https://www.teachingcouncil.ie/assets/uploads/2023/09/guidance-for-registered teachers-about-the-use-of-social-media-and-electronic-communication.pdf

The AUP guidance template allows schools to determine whether the use of social media sites and online forums is allowed, restricted or not permitted, reflecting the age of students and local context.

Acceptable Use Policy - Safeguards against age-inappropriate content and platforms

Schools are advised to apply technical safeguards, including broadband filtering and monitoring of internet usage, to minimise exposure to inappropriate material. Students must not intentionally access material that is obscene, illegal, harmful or otherwise objectionable and are encouraged to report accidental access.

Child protection procedures

The Child Protection Procedures for Schools 2025 requires schools to address online safety explicitly in their Child Safeguarding Statement and risk assessment. The Child Safeguarding Statement must identify the risks associated with access to the internet by children and set out the policies and procedures that are in place to manage these risks.

The Child Protection Procedures for Schools 2025 note the 2019 addendum to Children First - National Guidance for the Protection and Welfare of Children 2017, which highlights that while children and young people are often confident and competent users of new technologies, they may be less aware of the inherent risks involved. Children First operates under the premise that it is the responsibility of everyone in society to keep children and young people safe from harm.

The procedures are available at:

- www.gov.ie/en/department-of-education/policy-information/child-protection procedures-in-schools/

Cineáltas – preventing and addressing bullying including online safety

Cineáltas: The Action Plan on Bullying is the Department of Education and Youth's whole of education approach to preventing and addressing bullying behaviour in schools. The plan incorporates each of the nine components of UNESCO's Whole Education Approach to prevent and address bullying behaviour.

The Cineáltas: Action Plan on Bullying Implementation Plan 2023-2027 was published on 10 April 2023 and commits to implementing each of the 61 Actions contained in Cineáltas within a 5-year period. A number of actions relate to online safety.

The Cineáltas Action Plan and Implementation Plan are available at:

- www.gov.ie/en/department-of-education/publications/cinealtas-action-plan-on bullying/

Data protection in schools

The Data Protection Commission (DPC) is the national independent authority responsible for upholding the fundamental right of individuals to have their personal data protected. It is the supervisory authority responsible for monitoring the application of the General Data Protection Regulations (GDPR). The statutory powers, duties and functions of the DPC are as established under the Data Protection Act 2018.

The responsibility for compliance with data protection legislation rests with each school board of management. Schools/Education and Training Boards are separate data controllers from the department under data protection law and are responsible for their own compliance with the GDPR and Data Protection Act. Schools can consult with their management body and/or the Data Protection Commission (DPC) if they require further advice.

The DPC recently published a "Data Protection Toolkit for Schools" to assist with specific concerns and challenges faced by schools and following consultation with a number of organisations in the education sector. The Toolkit includes guidance on the use of technology in schools, including the arrangements of third-party service providers.

The DPC toolkit is available at:
www.dataprotection.ie/en/dpc-guidance/data-protection-toolkit-schools

Schools broadband – online content filtering

The department invests an average of €15m annually for the provision of broadband connectivity to schools. Under its Schools Broadband Programme at least 99% of recognised primary, special schools and post-primary schools are included in this programme.

HEAnet, Ireland's National Research and Education Network, provides high-speed internet connectivity and ICT shared services to all levels of the Irish education sector. They deliver and manage the Schools Network, through which they provide the actual network connection and includes content filtering and firewall security to schools on the network.

The purpose of content filtering is to ensure that inappropriate websites and content are not accessible from within schools using the school's broadband. Within the content filtering service provided, schools have the autonomy to choose between six different levels of content filtering so that they can choose a level that best meets their particular situation, for example, age group of students.

Content filtering systems classify websites into different 'categories', and these categories are used to control which category of website is allowed for schools on the different filtering levels. Level one is the most restrictive, while level six is the 'widest' level available as it allows access to websites such as YouTube, personal blogging and social networking. It should be noted that all six levels block access to inappropriate material in categories such as pornography and violence.

For information and advice on content filtering visit:

- www.oidetechnologyineducation.ie/content-filtering

Cybersecurity for schools

It is recognised that cybersecurity is an increasingly important concern for schools. To address this Oide Technology in Education (Oide-TiE) have developed a wide range of cybersecurity guidance and resources for schools.

Details of available supports can be found on the Oide-TiE Data Security Hub for Schools at:

- www.oidetechnologyineducation.ie/technology-infrastructure/data-security

Where you can access the following:

- A 'Quick Guide-Cybersecurity for schools' developed by Oide-TiE in partnership with the National Cybersecurity Centre (NCSC)
- Cybersecurity Readiness Guide for your School
- A School Cybersecurity Policy Template
- Authentication/Access Policy Guide and Template
- Cybersecurity Incident Response and Recovery Guide
- Cybersecurity Awareness and Training for School Leaders
- Cybersecurity FAQs

If you need cybersecurity advice or support, please email:

- ictadvice@oide.ie