DIXONS
ACADEMIES
TRUST

Online Safety Policy and Acceptable use of Information Technology

Online safety and acceptable use of technology policy: document provenance

Approver	School and college trust leaders
Date of approval	February 2026
Policy owner	School and college trust leader: Business Services
Policy authors	Head of IT Centre of Excellence
Version	2.0
Date of next review	September 2027
Summary of changes in this review	• Section 15 added to introduce the use of DAT devices is allowed to bring it in line with previous GAET acceptable use policy
Related policies and documents	• Anti-Bullying Policy • Child Protection Policy (incorporating Keeping Children Safe In Education) 2020) • Positive Behaviour Policy • Professional Conduct Policy • Academy-Home Contract • Keeping Children Safe in Education • Relationship and Sex Education Programme of Study (academy website) • GDPR / Data Protection

Unless there are legislative or regulatory changes in the interim, the policy will be reviewed as per the review cycle. Should no substantive change be required at this point, the policy will move to the next review cycle.

Contents

1.0 Policy statement

Dixons Academies Trust recognises that if used correctly, technology can support and greatly enhance learning and communication. The use of technology can support the acquisition of powerful knowledge and encourage student independence. As an organisation, the use of technology facilitates healthy and efficient communication and the sharing of ideas within and beyond our academies. All members of our organisation must understand what is meant by appropriate and inappropriate use of technology and the responsibility that comes with access to shared resources, including the internet. Staff and students alike must appreciate that there can be risks and possible threats associated with online communication and that there is a clear expectation of conduct.

Given that technology has blurred the boundaries of community, everyone must be mindful at all times of how their online conduct could negatively impact on others. Dixons Academies Trust is a values-driven organisation with highly professional relationships and diversity at its heart; we take seriously any wilful or unwitting damage to members of our community, or our reputation, caused by careless digital communication. In alignment with the Keeping Children Safe In Education guidance, Dixons Academies Trust is committed to an effective whole-school approach to online safety, ensuring all stakeholders are protected and educated in their use of technology and that robust mechanisms exist to identify, intervene in, and escalate any online safety concerns.

2.0 Scope and purpose

This policy covers all individuals, both students and staff working at all levels in the organisation, including ambassadors, executives, principals, senior leadership, all teaching and associate staff, casual and agency workers (collectively referred to as employees or staff).

The policy should be read in conjunction with the following policies / documents:

- Anti-Bullying Policy
- Child Protection Policy (incorporating Keeping Children Safe In Education 2025)
- Positive Behaviour Policy
- Professional Conduct Policy
- Academy-Home Contract
- Keeping Children Safe in Education
- Relationship and Sex Education Programme of Study (academy website)
- GDPR / Data Protection

Online safety covers the use of online platforms such as Microsoft Teams, the Internet (~~and~~ in particular social media) and also the use of mobile phones and other electronic communication technologies. If a member of staff is at all unsure as to whether an activity is a crime, they should refer to the National Police Chief's Council document. Refer particularly to the cyber-crime flow chart.

3.0 Roles and responsibilities

This policy has been reviewed by the school and college trust leaders the designated safeguarding leads cross-cutting team and the IT cross-cutting team: it has been formally adopted by the trust board. Trustees delegate responsibility for the application of the policy to the principal and senior leadership of each academy and hold the principal to account for ensuring online safety and appropriate use of IT is given primacy both with staff and students.

3.1 Trustees

Trustees review the data which includes a category on inappropriate online activity. In this way they are testing the application of the policy. The safeguarding trustee ensures that:

- an online safety policy is in place, reviewed every year and / or in response to an incident and is available to all stakeholders
- the DSL has overall responsibility for online safety of students and that this is in their job description
- procedures for the safe use of ICT and the Internet are in place and adhered to
- the principal and staff are accountable for online safety

3.2 Principal and senior leadership team (SLT) including the designated safeguarding lead (DSL)

The principal has a duty of care for ensuring the safety (including online safety) of members of the community, day-to-day responsibility for online safety is delegated to the designated safeguarding lead who works with middle leaders in making sure there is a proactive programme of education in place. Any complaint about staff misuse must be referred to the principal.

The principal will work with the DSL in ensuring that:

- all staff receive regular, up to date training both in educating young people, but also in relation to their own online conduct

- regularly reviews the online programme of study for young people by undertaking the 360 degree review
- appropriate action is taken in all cases of misuse
- internet filtering methods are appropriate, effective and reasonable, reporting any issues immediately to the head of IT
- GDPR and data protection duty is taken seriously
- issues of inappropriate use of IT are monitored and that policies and training are reviewed as appropriate
- reports online safety issues to the trustees through the safeguarding link trustee

3.3 Dixons head of IT Centre of Excellence

The head of IT Centre of Excellence is responsible for ensuring that:

- our trust's technical infrastructure is secure and is not open to misuse or malicious attack
- the online safety policy is relevant and reflects risks associated with new technology
- users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant.
- the use of all aspects of the network is regularly monitored in order that any misuse or attempted misuse can be reported to the principal for investigation
- monitoring software and systems are implemented and updated regularly

4.0 Potential harm to children and duty of care

4.1 We know that some adults and young people will use technology to harm others, particularly if they perceive a vulnerability. The breadth of issues associated with online safety is considerable but can be classified into four main areas of safeguarding risk:

Content: being exposed to illegal, inappropriate or harmful material for example, pornography, fake news, racism, misogyny, suicide, anti-Semitism, radical extremism, misinformation, disinformation (including fake news) and conspiracy theories.

Contact: being subjected to harmful online interaction with other users for example, peer to peer pressure, inappropriate age-inappropriate adverts, adults posing as children or young adults, sexual or criminal grooming or financial exploitation.

Conduct: personal online behaviour that increases the likelihood of, or causes harm, for example, making, sending or receiving explicit messages or images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and / or pornography, sharing other explicit images and online bullying.

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

4.2 As well as being used as a form of, or prelude to abuse, electronic communication can be used to intentionally polarise positions leading to young people feeling excluded or isolated. We are aware that young people often cite social media as a cause of anxiety. More recently, research has increasingly begun to explore the harmful effects of social media for example on body image and self-esteem, social isolation and depression. As such, social media may have a negative effect on young people's mental health.

4.3 There is a duty of care for all employees to educate the young people in our care on the risks and responsibilities associated with the use of technology. In all our academies, education on online safety happens in; IT lessons, Personal, Social, Health Education and assemblies. Sometimes other agencies such as the police may come in to support the programme of education. All education is age-appropriate and specific to the experience of the young person at a particular stage in their development. Teachers should never underestimate the importance of taking the opportunity to educate as the moment arises, for example a high profile case.

4.4 This policy aims to be an aid in regulating activity and supporting the education of conduct online both inside and outside of academy hours. Online safety is a whole-school issue and is everyone's responsibility.

4.5 As well as protecting and educating young people, it is vital that they understand that actions have consequences and that inappropriate use of IT to harm others, will not be accepted. Every academy has a table of sanctions that relates to their specific approach to managing behaviour and reference is made to inappropriate use of IT. Students must be mindful that purposefully harming any member of our community or expressing views which could bring individuals or our organisation into disrepute, will not be tolerated.

5.0 Staff and appropriate use of IT and social media

5.1 Not only do all staff have a duty of care towards young people, they are also duty-bound as professionals to use IT appropriately both within and beyond the organisation. In the same way as there can be consequences for young people, there can be for staff and we regularly train on being mindful of your 'digital footprint'—the permanent record created by emails, messages, posts, comments, images, and online activity that may be stored, shared, or retrieved in the future—and ensuring communication meets the 'red face test', meaning staff should consider whether they would feel comfortable and professionally confident if the content were made public, shared with parents, colleagues, senior leaders, or reported in the media. Our staff understand that any apparently private digital communication can become public and if it does, this could cause them or the organisation considerable embarrassment.

5.2 Appropriate conduct on social media is referenced in the Professional Conduct policy and also in part two of the Teachers' Standards. It is not expected that any employee will digitally communicate anything that could bring their profession or the organisation into disrepute.

5.3 Any views expressed on X (formerly Twitter) or LinkedIn for example, must make clear that they are the employees own and should still not lead to a reputational risk through association. Employees must be aware that digital communication can be misunderstood and / or misquoted and may lead to misunderstandings that could put them at risk of allegation. For those who work with children or young people, Keeping Children Safe in Education makes clear that an allegation may be made against someone if they have 'behaved or may have behaved in a way that indicates they may not be suitable to work with children'. This includes online behaviour that may occur inside or outside of the place of work.

5.4 Staff are clear that they should never communicate with students on social media, by personal text or by any online platform other than those used legitimately in the academy and only ever in relation to learning.

6.0 Making use of IT to enhance learning and improve communication

The internet and online platforms are used in all our academies to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance communication. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary IT skills that they will need to enable them to progress confidently onto university or a real alternative when they leave Dixons.

Some of the benefits of using IT including the internet are:

6.1 For students:

- unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries
- access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet
- an enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen
- access to learning whenever and wherever convenient
- freedom to be creative
- freedom to explore the world and its cultures from within a classroom
- social inclusion, in class and online
- access to case studies, videos and interactive media to enhance understanding
- individualised access to learning
- supervised and appropriate access to the internet within a classroom provides the opportunities students need to learn to keep themselves safe and behave responsibly online

6.2 For staff:

- professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies
- immediate professional and personal support through networks and associations
- improved access to technical support
- ability to provide immediate feedback to students and parents
- class management, attendance records, schedule, and assignment tracking

7.0 Evaluating internet content

7.1 With so much information available online it is important that students learn how to critically evaluate information. Students will be taught to:

- be critically aware of materials they read, and shown how to validate information before accepting it as accurate

- use age-appropriate tools to search for information online
- acknowledge the source of information used and to respect copyright. Plagiarism is against the law and any intentional acts of plagiarism are taken very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam and or the full series

7.2 All our academies have internet filters to ensure that content is appropriate to the age and maturity of students. If staff or students discover unsuitable sites, then the URL will be reported to the designated safeguarding officer. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular checks will take place to ensure that filtering services are working effectively.

7.3 The trust delivers regular onsite safety education to pupils and staff, addressing the 4Cs, reporting mechanisms, responsible use, and the evolving nature of online risks. Induction for new staff also includes online safety guidance and awareness of monitoring and filtering.

7.4 Staff regularly receive training to reinforce the mechanisms to report safeguarding concerns, particularly around the use of CPOMS to record information and the role of DSLs to whom Senso will also automatically flag concerns based on user interaction. Students are also given lots of education and reinforcement about the importance of telling a trusted adult if they feel unsafe, see something dangerous or which makes them uncomfortable or if they need any help. Academies are responsible for implementing a variety of reporting mechanisms to enable students to report any concern.

8.0 Emails

All our academies use email internally for staff and students and externally for contacting parents and outside agencies, particularly in the case of potential safeguarding matters; it is an essential part of our communication and can often provide an important paper trail.

Staff and students are aware that Dixons email accounts should only be used for work-related matters. Our trust has the right to monitor emails and their contents and in the case of a subject access request, emails will be produced and shared, unless there would be a specific safeguarding reason that would prohibit this.

8.1 Staff should be aware of the following when using their academy email address:

- they should only use official school-provided email accounts to communicate with students, parents or carers. Personal email accounts should not be used to contact any of these people
- emails sent from a Dixons account should be professionally and carefully written. Staff are always representing our trust and should take this into account when entering into any email communications
- they must tell their line-manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the academy or from an external account. They should not attempt to deal with this themselves.
- the forwarding of chain messages is not permitted

8.2 Students should be aware of the following when using email in school, and will be taught to follow these guidelines through the IT curriculum and in any instance where email is being used within the curriculum or in class:

- in the academy they should only use school-approved email accounts
- they should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the academy or from an external account. They should not attempt to deal with this themselves
- they must be careful not to reveal any personal information over email or arrange to meet up with anyone who they have met online without specific permission from an adult in charge

Students will be educated to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

9.0 Social networking, social media and personal publishing

9.1 Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are potentially more vulnerable to content, contact and conduct behavioural issues. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online. Students are not allowed to access social media sites in any of our academies and we do not allow the use of mobile phones.

9.2 Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught this through the IT curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in the public domain. All our academies teach the following general rules on the use of social media and social networking:

- students are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the expected code of conduct regarding the use of IT and technologies and behaviour online

- they are taught in age-appropriate way about the possible safeguarding dangers of online communication
- any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use, additionally our online filter (FortiGate) blocks inappropriate sites and searches
- in areas where we have IT equipment we use a system (Senso) to monitor student searches and IT use.
- students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory
- students and staff are warned against sharing or liking seemingly harmless messages which may have been shared by extremist organisations
- the trust expects all staff and pupils to remember that they are always representing their academy and must act appropriately and in line with our very clear values
- safe and professional behaviour of staff online will be discussed at staff induction and is referred to in the Professional Conduct policy and Teachers' Standards

9.3 Filtering must block and flag access to high-risk categories (including adult content, extremism, self-harm, suicide, hate speech, gambling, phishing, misinformation, disinformation and conspiracy theories.) Monitoring systems must also detect searches or behaviours which indicate risk to the above categories.

10.0 Mobile phones and personal devices

10.1 Students

- Students who breach this policy in relation to the use of personal devices will be disciplined in line with the behaviour policy. Their mobile phone will be confiscated.
- Under no circumstances can a student bring mobile phones or personal devices into examination rooms with them. If a student is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in them being prohibited from taking that exam or having their grades cancelled.

10.2 Staff

- Under no circumstances should staff give their personal number or email address to parents or students.
- Staff must have permission to take photos or videos of pupils and should not store these on any personal device.
- Our trust expects staff to lead by example. Personal mobile phones should be switched off, out of view or on 'silent' whenever possible, unless they are being used for a specific work purpose.
- Any breach of the policy may result in disciplinary action against the member of staff. More information on this can be found in the child protection and safeguarding policy, the disciplinary policy and dealing with allegations against members of staff along with the staff contract of employment.

12.0 Cyberbullying

12.1 Cyberbullying is a distinct form of bullying that exists within the broader definition due to its expansive reach; it may occur at any hour and potentially affect a wide audience. Furthermore, it often transpires off academy premises and outside regular academy hours. Internet anonymity can lead individuals to express or engage in behaviour online that they might refrain from in face-to-face interactions._Furthermore, the artefacts of cyberbullying, including things like youth produced sexual imagery or abusive comments, have the potential to travel to any other point in the world and there are few or no options to limit or retract once information has been shared in this way.

12.2 As with all forms of bullying, cyberbullying is a form of child on child abuse, as defined by Keeping Children Safe in Education. The terms 'bullying' and 'cyberbullying' are commonly used to describe these behaviours and its meaning is established in both education and society in general, but using it can lead to minimisation of the seriousness of the behaviour if not also understood as a safeguarding concern for both the perpetrator(s) and victim(s) involved.

12.3 Cyberbullying has become the most common form of bullying that education now faces. We believe that any act of harmful behaviour that occurs between members of our school community is our business and will be managed within the remit of our policies and routines.

12.4 Any allegation or observation of potential cyberbullying will be taken seriously and acted upon promptly, in line with our Anti-bullying, Positive Behaviour, and Safeguarding and Child Protection policies, as well as the academies' own routines and processes.

12.5 Not all cyberbullying is criminal or meets statutory thresholds for referral to Children's Social Care, but there are laws that can apply in relation to threats, harassment and the safeguarding of children, and so the police or other services will be involved as and when necessary. The Education Act 2011 gives head teachers, and those authorised by head teachers, the power to seize and examine data or files and to delete these where there is good reason to do so.

13.0 Managing emerging technologies

Technology is progressing rapidly, and new technologies are emerging all the time. The head of IT will support the executive in risk-assessing any new technologies before they are allowed in to our academies and will consider any educational benefits that they might have. We are always conscious of the risks that new technology may attract, for example the use of Microsoft Teams, however, we also do not want to inhibit our students' learning by not allowing them access to the most up to date platforms.

13.1 Use of removable media

- To protect our systems and data, staff and students must not use unauthorised removable media such as USB memory sticks or external hard drives on the trust devices or the trust network. Trust data must only be stored in approved locations such as Microsoft Teams, SharePoint and OneDrive, in line with our data protection and information security guidelines.
- Any exception to this restriction, for example to aid staff in the support of student examinations and the storage of marked assessments, must be risk assessed and approved by the Head of Data Governance and Head of IT to ensure that it is appropriately encrypted and managed.

14.0 Delivering online lessons

As a result of our experience of an international pandemic, as a trust, we have started to deliver online lessons. Synchronous (real-time video conferencing) poses more of a risk than asynchronous (e.g. setting work via a VLE), however, both deliveries need to be considered from a safeguarding perspective. It is absolutely vital that clear protocols are adhered to in order to minimise potential safeguarding issues. The academy must have a home-school agreement specifically related to online lessons (see appendix below) which explains the role of the academy, the expectation of the student and the expectation of the parent. All online lessons must be timetabled in the same way that physical lessons are and the principal must know when lessons are occurring. No change of time should be made without agreement from the SLT and the parent. In the agreement there should be reference to where lessons should take place and the importance of maintaining professionalism and an appropriate teacher-student relationship. There will be a clear expectation of conduct as there is in the classroom and also a dress code. The environment should be kept as formal as possible and no informality of communication should be allowed to develop. Teachers need to be aware that online material can be published in a way in which it is not intended and remain vigilant to malicious publishing of videos that could bring the individual and the academy into disrepute. No teacher will deliver online lessons without full safeguarding and behaviour management training.

15.0 Use of Dixons devices off-site

As part of our commitment to ensuring students have access to high-quality learning opportunities, Dixons devices may be used off-site, including within the home environment, provided that appropriate safeguarding, filtering and monitoring controls are in place.

Our trust's technical controls, including mandatory filtering and monitoring systems, must remain installed, active and unaltered at all times. Where devices are used beyond our academies, students and parents/carers must ensure that:

- the device is used responsibly and only for educational purposes;
- the safeguarding and monitoring software deployed by the trust is functioning and has not been removed, disabled or bypassed;
- any concerns relating to online safety, misuse or technical issues are reported promptly to the academy.

All expectations outlined in this policy apply equally to device use both inside and outside academy hours. Our trust reserves the right to review, monitor and audit activity on any Dixons device—whether used on-site or off-site—to ensure compliance with safeguarding, security and acceptable use requirements.