



# One Degree Academy

## ONLINE SAFETY & ICT POLICY

Author	GCO
Date Ratified	Sept 2023





## ODA Online Safety and ICT Policy

support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good online safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

Online safety covers the internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any person working with children and educating all members of the school community on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. Online safety is a whole-school issue and responsibility.

Cyber-bullying by students will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures which are outlined in our behaviour policy.

### 1. Communicating school policy

This policy is available on the school website for parents, staff, and students to access when and as they wish. Rules relating to the school code of conduct when online, and online safety guidelines, are displayed around the school. Online safety is integrated into the curriculum in any circumstance where the internet or technology are being used.

### 2. Making use of ICT and the internet in school

The internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. 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 ICT skills that they will need in order to enable them to progress confidently into their next stage of education and beyond.

Some of the benefits of using ICT and the internet in schools are:

- **For students:** Unlimited access to worldwide educational resources, research tools and institutions such as art galleries, museums and libraries.
- Access to subject experts, role models, inspirational people and organisations. 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.

## ODA Online Safety and ICT Policy

- 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.

### 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.
- Communication with all stakeholders

### 3. Learning to evaluate internet content

With so much information available online it is important that students learn how to evaluate internet content for accuracy and intent. This is approached by the academy as part of digital literacy across all subjects in the curriculum. Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- to use age-appropriate tools to search for information online
- what to do to safeguard themselves online including what to do if they feel unsafe online

The academy will also take steps to filter internet content to ensure that it is appropriate to the age of the students. If staff or students discover unsuitable sites then the URL will be reported to the *academy online safety coordinator* . Any material found by members of the academy community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

### 4. Managing information systems

The academy is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of academy data and personal protection of our community very seriously. This means protecting the academy network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the academy information systems and users will be reviewed regularly by the network manager and virus protection software will be updated regularly. Some safeguards that the academy takes to secure our computer systems are:

- ensuring that all personal data sent over the internet or taken off site is encrypted
- making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this

## ODA Online Safety and ICT Policy

- files held on the school network will be regularly checked for viruses
- the use of user logins and passwords to access the academy network will be enforced
- portable media containing academy data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.

For more information on data protection in school please refer to our data protection policy.

### 5. Emails

The academy uses email internally for staff and for contacting parents, and is an essential part of school communication

Staff are aware that academy email accounts should only be used for academy-related matters. This is important for confidentiality. The academy has the right to monitor emails and their contents but will only do so if it feels there is reason to.

#### 5.2 School email accounts and appropriate use

**Staff should be aware of the following when using email in school:**

- Staff should only use official academy-provided email accounts to communicate with parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
- Emails sent from academy accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Staff must tell their 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.

**Students should be aware of the following when using email in the academy,** and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class: Students will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing. One Degree may choose to limit the use of email for students until such learning has taken place.

### 6. Published content and the academy website

The academy website is viewed as a useful tool for communicating our ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with academy news and events, celebrating whole-school achievements and personal achievements, and promoting academy projects.

## ODA Online Safety and ICT Policy

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or students will be published, and details for contacting the academy will be for the school office only.

### 7.2 Policy and guidance on safe use of children's photographs and work

Colour photographs and students work bring our school to life, showcase our student's talents, and add interest to publications both online and in print that represent the academy. However, the academy acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the General Data Protection Regulation 2016 images of students and staff will not be displayed in public, either in print or online, without consent. On admission to the academy parents/carers will be asked to sign a photography consent form. The academy does this so as to prevent repeatedly asking parents for consent over the year, which is time-consuming for both parents and the academy. The terms of use of photographs never change, and so consenting to the use of photographs rather than a one-off incident does not affect what is being consented to. This consent form will outline the school's policy on the use of photographs of children.

#### Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. The academy is careful to ensure that images published on the academy website cannot be reused or manipulated. Only images created by or for the academy will be used in public and children may not be approached or photographed while in the academy or doing school activities without the academy's permission. The academy follows general rules on the use of photographs of individual children:

- Parental consent must be obtained. Consent will cover the use of images in:
  - all academy publications
  - on the academy website
  - in newspapers as allowed by the academy
  - in videos made by the academy or in class for projects.
- Electronic will be stored securely.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed. Photographs of activities that may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the students (ie a student in a swimming pool, rather than standing by the side in a swimsuit).

## ODA Online Safety and ICT Policy

- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or class name.
- Events recorded by family members of the students such as school plays or sports days must be used for personal use only.
- Students are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the academy will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the students. For more information on safeguarding in school please refer to our school child protection and safeguarding policy.

### 6.3 Complaints of misuse of photographs or video

Parents should follow standard academy complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our complaints policy for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the academy's child protection and safeguarding policy and behaviour policy.

### 6.4 Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. 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 the academy and there are various restrictions on the use of these sites in the academy that apply to both students and staff.

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 through the ICT curriculum about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The academy follows general rules on the use of social media and social networking sites in school:

- 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 academy's code of conduct regarding the use of ICT and technologies and behaviour online.
- 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.
- Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.

## ODA Online Safety and ICT Policy

- Students and staff are encouraged not to publish specific and detailed private thoughts that might be considered hurtful, harmful or defamatory. The academy expects all staff and students to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

### 7. Mobile phones and personal device

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:

- they can make students and staff more vulnerable to cyberbullying
- they can be used to access inappropriate internet material
- they are valuable items that could be stolen, damaged, or lost
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.
- Student mobile devices should not be carried into the school building without prior permission. This is requested in writing and needs to be agreed by SLT and will be granted dependent on age and circumstances
- Agreed mobile devices are to be handed in on entry to the building and stored securely to be picked up at the end of the day. Non-agreed mobile devices will be confiscated and parents notified
- If there is reason to believe that there may be evidence of harmful or inappropriate use on a device, the device will be confiscated by a member of staff and the device can be searched. If evidence is found relating to any safeguarding concerns or to unlawful behaviour the device may need to be shared with outside agencies e.g. police, MASH team etc. In these circumstances the academy will take direction from these outside agencies as requested
- The academy will not take responsibility for personal devices that have been lost, stolen, or damaged

### 8.2 Mobile phone or personal device misuse

#### Students

- Students who breach academy policy relating to the use of personal devices will be disciplined in line with the academy's behaviour policy. Students, if found with a mobile device, will have their device confiscated. Parents will be notified and the device will be returned up to 3 weeks later.
- The academy will not tolerate cyberbullying against either students or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the school's disciplinary sanctions read the school behaviour policy.

## ODA Online Safety and ICT Policy

### Staff

- Use of personal devices is permitted at the academy; however, this is strictly regulated and must be done in accordance with this policy
- To minimise any risks, all personal mobiles must not be used where children are present.
- Under no circumstances should staff members or visitors make or receive personal phone calls or texts or use their phone as a camera where children are present to ensure potential risks are minimised.
- Members of staff bringing personal devices into the academy will ensure that there is not any inappropriate or illegal content on their device and must ensure that their devices are password-protected, and insured. The academy will not be held responsible for any loss, theft or damage of personal mobile phones.
- Under no circumstances are images, videos or audio recordings to be made on personal devices without prior explicit written consent by the designated safeguarding person.
- Personal mobiles may be used in designated areas at break times (staffroom, academy offices and car park area outside the academy building).
- Staff are advised to provide their work place contact number to their family members, own children's schools/academies for use in the event of an emergency.
- Under no circumstances should staff use their own personal devices to contact students or parents either in or out of school time. This includes when there is a pre-existing relationship outside of school and the staff member is phoning about a school matter.
- The academy expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours as per the code of conduct.
- Any breach of academy policy may result in disciplinary action against that member of staff. More information on this can be found in the child protection and safeguarding policy, or in the staff contract of employment.
- Visitors, including other professionals, contractors and parents/carers are made aware by the visitor agreement and verbal reinforcement that they are not to use their mobile phone where children are present.

### 8. Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the academy. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the behaviour policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the academy community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

If an allegation of bullying does come up, the school will:

- take it seriously
- act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the students involved
- record and report the incident





## ODA Online Safety and ICT Policy

- provide support and reassurance to the victim
- make it clear to the students involved that this behaviour will not be tolerated. If there is a group of students involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the academy will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the student(s) will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in school.

Repeated incidents may result in a fixed-term exclusion.

### 9. Managing emerging technologies

Technology is progressing rapidly and new technologies are emerging all the time. The academy will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The academy keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

### 10. Protecting personal data

One Degree Academy believes that protecting the privacy of our staff and students and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from students, parents, and staff and processes it in order to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

Under the General Data Protection Regulation 2016, and following principles of good practice when processing data, the school will:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights

## ODA Online Safety and ICT Policy

- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the academy is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school's safeguards relating to data protection read the school's data protection policy.

### **11. Filtering and Monitoring**

ODA staff and governors understand what filtering and monitoring is, and are aware that it is in place to prevent children accessing inappropriate and harmful content online while students are in the academy. The DSL will take lead responsibility for understanding the filtering and monitoring systems in place at the academy and all staff are informed of changes in their safeguarding training. The DSL along with the IT lead/IT providers and Safeguarding governor will work closely to ensure all filtering and monitoring standards are adhered to. The DSL will also schedule regular filtering and monitoring reviews to ensure we are compliant. The DSL along with the IT lead/IT provider will use adaptable filtering to ensure all harmful and inappropriate content is blocked without unreasonably impacting teaching and learning. The DSL will deliver regular CPOMS training where staff are trained on how to spot concerns online and respond appropriately. When a third party/external organisation uses One Degree Academy's IT equipment, the academy's procedures should be followed and appropriate referrals to external agencies made if necessary.

