

January | 18

Unity Academy Trust Acceptable Usage Policy

Rationale

Unity Academy Trust's (UAT) ICT and communications systems are intended to promote effective communication and working practices. This Policy outlines the standards members, trustees, local governors and employees must observe when using these system, when UAT will monitor their use, and the action UAT will take if these standards are breached.

This Policy is to be used in conjunction with other UAT Policies including any Social Media Policy.

UAT is committed to ensuring that this Policy and its application reflect the UAT Equal Opportunities at Work Policy. This means treating people fairly regardless of their colour, race, ethnic or national origin, language, religion or belief, gender or gender reassignment, marital status, sexuality, disability, age, or any illness or infection. In particular, UAT recognises its responsibility to meet all its legal obligations for managing employees with underlying health issues in line with the Equality Act 2010 (Disability) (previously under the Disability Discrimination Act (1995)).

The Policy and Procedure applies to all employees and volunteers within CGS Trust. The Policy and Procedures may be amended from time to time by the Executive Headteacher and/or Trustees, in order to reflect changes in statutory requirements or organisational arrangements.

Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

Acceptable Use Statement

The computer system is owned by the school. "The computer system" means all computers and associated equipment belonging to the school, whether part of the school's integrated network or stand alone, or taken offsite.

Professional use of the computer system is characterised by activities that provide children with appropriate learning experiences; or allow adults to enhance their own professional development. The school recognises that technologies such as the Internet and e-mail will have a profound effect on childrens education and staff professional development in the coming years and this policy has been drawn up accordingly.

The installation of software or hardware unauthorised by the school, whether legitimately licensed or not is expressly forbidden.

The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited.

All members of staff, students on placement, supply teachers etc must sign a copy of this policy statement before a system login password is granted. All children must be made aware through class discussion of all the important issues relating to acceptable use, especially the monitoring of Internet use.

Internet Access Policy Statement

- All Internet activity should be appropriate to staff professional activities or the children's education;
 - Access is limited to the use of authorised accounts and passwords, which should not be made available to any other person;
 - The Internet may be accessed by staff and children throughout their hours in school;
 - Activity that threatens the integrity of the school's computer systems, or that attacks or corrupts other systems, is prohibited;
 - Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received. Due regard should be paid to the content. The same professional levels of language should be applied as for letters and other media;
 - Use of the school's Internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is excluded;
 - Copyright of materials must be respected. When using downloaded materials, including free materials, the Intellectual Property rights of the originator must be respected and credited. All material saved on the school's network is the property of the school and making unauthorised copies of materials contained thereon maybe in breach of the Data Protection Act, Individual Copyright or Intellectual Property Rights;
 - Use of materials stored on the school's network for personal financial gain is excluded;
 - Posting anonymous messages and forwarding chain letters is excluded;
 - The use of the Internet, e-mail, or any other media to access inappropriate materials such as pornography, racist or any other offensive material is forbidden;
 - Children must not be given unsupervised access to the Internet. For the purposes of this policy, `supervised` means that the user is within direct sight of a responsible adult;
 - The teaching of Internet safety is included in the school's ICT Scheme of Work, but all teachers within all year groups should be including Internet safety issues as part of their discussions on the responsible use of the school's computer systems;
 - All children must understand that if they see an unacceptable image on a computer screen, they must turn the screen off and report immediately to a member of staff.
- **System Monitoring**
- Through the LGfL and the school's Google Apps account, all internet activity is monitored by the system. It is the responsibility of the Administrator to review this activity periodically. It is the duty of the Administrator to report any transgressions of the school's Internet policy and/or use of obscene, racist or threatening language detected by the system to the ICT coordinator &/or the Headteacher. Occasionally, it may

be necessary for the Administrator to investigate attempted access to blocked sites, and in order to do this, the Administrator will need to set his/her Internet access rights to `Unrestricted`. Whenever this happens, this should be recorded in the ICT violations register, and the Headteacher notified;

- All web activity is monitored, including the content of e-mail, therefore it is the responsibility of the user to ensure that they have logged off the system when they have completed their task;
- All serious transgressions of the school's Internet Access Policy are recorded in the school's ICT violations register. The violations register can be found in the subject coordinator's file;
- Transgressions of Internet Policy and use of inappropriate language can be dealt with in a range of ways, including removal of Internet access rights; computer system access rights; meetings with parents or even exclusion; in accordance with the severity of the offence and the school's Behaviour Policy;
- Breaches of Internet Access Policy by staff will be reported to the Headteacher and will be dealt with according to the disciplinary procedures, or through prosecution by law.

- **Internet Publishing Statement**

- The trust wishes that schools' web sites reflect the diversity of activities, individuals and education that can be found at each school. However, UAT recognises the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the Internet, the following principles should be borne in mind:
- No video recording or photographed image may be published without the written consent of the parents/carers or legal guardian of the child concerned, and the child's own verbal consent;
- Surnames of children should never be published, especially in conjunction with photographic or video material;
- No link should be made between an individual and any home address (including simply street names);
- Where the person publishing material suspects that there may be child protection issues at stake then serious consideration must be taken as to whether that material may be published or not. In the case of a simple piece of artwork or writing, this may well be fine, but images of that child should not be published. If in any doubt at all, refer to the person responsible for child protection;
- Adults are encouraged to set up blogs and other online environments to celebrate and stimulate learning. Blogs should be set up by adults and controlled from an adult's Google apps account only. Children should be allowed to contribute to the blog under adult supervision. Adults should carefully monitor all comments before approving them to be published. Children are not permitted to set up their own blogs, or access their personal blogs in school;

Social Media and Electronic Communication

- Social Media: staff are encouraged to make use of social media for their own development. Use of social media in school is permitted only within the definition of the 'professional use' statement above.
- Children should be supervised at all times when accessing and using school or class social media accounts. Children are not permitted to access their own social media accounts in school.
- Staff are advised in the strongest terms not to make connections on social media websites with pupils at the school, or to other adults who have connections with pupils within the school. Staff are advised to review the security settings on their social media accounts and to seek advice about this from their union.
- Electronic communications with pupils: Unity Academy Trust recognises the role that the internet and associated electronic communications can play in developing a 21st century curriculum. As part of this, teachers and pupils may communicate electronically. Staff should only communicate electronically with a pupil in an open forum, i.e. a forum that can be viewed publically. This might include, but is not limited to discussion forums, the comments section of a blog, an @user message on twitter or an online pin board. It is expressly forbidden for teachers to communicate privately with a student, for example through email or direct messaging.
- Google Drive. When working in the cloud, pupils should share their work with their group, their teacher and the monitoring address. Teachers may communicate electronically on a cloud document only when it is shared with at least two pupils and the monitoring account.
- Any emails sent from a school account must include the school's approved indemnity and privacy statement.
- *All of the above is in conjunction with the Social Media Policy adopted by the school.*

Off Site Usage

- Equipment such as laptop computers and iPads may be taken offsite for use by staff in accordance with the Acceptable Use Statement and Internet Access Policy. When school equipment is taken offsite, the member of staff who has taken it is wholly responsible for it and is liable for any loss or damage.
- Any costs generated by the user at home, such as phone bills, printer cartridges etc. are the responsibility of the user;
- Where a member of staff is likely to be away from school through illness, professional development (such as secondment etc.) or maternity leave,

arrangements must be made for any portable equipment in their care to be returned to school;

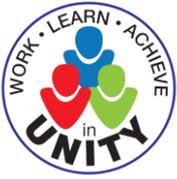
- If an individual leaves the employment of the school, any equipment must be returned;
- Staff may install software on laptops to connect to the Internet from home once agreed by a member of the Senior Leadership Team. If in doubt seek advice;
- No other software, whether licensed or not, may be installed on laptops in the care of teachers. The school does not own or control the licences for such software.

Use of personal devices

To comply with the principles of the Data Protection Act 2018, and the Trust's policy on data protection, when using a personal device to read or access school information, I agree to the following

- Staff are permitted to make use of personally owned devices in accordance with the description of 'professional use' stated above.
- Staff are reminded that the school cannot accept liability for the loss or damage of these devices and they are used entirely at the risk of their owner. Any ancillary costs such as app purchases for private devices or Internet connection charges are solely and entirely the responsibility of the owner.
- The use of private devices for the capture or storage of images or video of pupils is expressly forbidden.
- That If the device is lost, stolen or if you sell it, confidential information might be accessible to a third party; therefore I will notify the DPO immediately especially if it has google software on it.
- That if I cease to work for Unity Academy Trust all data will be deleted and removed from any device. Devices belonging to the Trust will be handed back upon ceasing employment or a voluntary role finishing.
- That if a personally owned device is used in an insecure manner, or used by another family member, I am in breach of transferring information to unrelated parties and could be sharing data with personal outside of the trust. I know I am duty bound to report this to the DPO.
- To only use encrypted devices, (USB keys, removable hard drives, and laptop) to save any data onto. These must be approved by the Trust's IT personnel.
- To not download any personal or sensitive information, relating to school onto any personal devices. i.e pupil data from any school system.
- All devices that I use must be locked after being left idle for no more than 5 minutes.

- That all passwords will be kept confidential and not shared with family or third parties.
- To ensure that anti-virus software is up to date on any device especially if logging onto wifi in public places as these may not be secure.



Declaration of Understanding.

- I confirm I have read and understood the Unity Academy Trust Acceptable Use Policy.
- Signed: _____
- Date: _____
- Name: _____ (please print)
- Role: _____
- Institution: Unity Academy Trust